

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/004099

International filing date: 09 March 2005 (09.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-106946
Filing date: 31 March 2004 (31.03.2004)

Date of receipt at the International Bureau: 20 May 2005 (20.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 4 年 3 月 3 1 日
Date of Application:

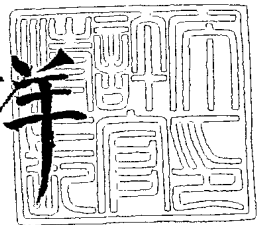
出 願 番 号 特 願 2 0 0 4 - 1 0 6 9 4 6
Application Number:
[ST. 10/C]: [J P 2 0 0 4 - 1 0 6 9 4 6]

出 願 人 オムロン株式会社
Applicant(s):

2 0 0 5 年 3 月 1 1 日

特許庁長官
Commissioner,
Japan Patent Office

小 川 洋



【書類名】 特許願
【整理番号】 62851
【提出日】 平成16年 3月31日
【あて先】 特許庁長官 殿
【国際特許分類】 B60R 25/00 606
B60R 25/04 602
B60R 25/04 608

【発明者】
【住所又は居所】 京都府京都市下京区塩小路通堀川東入南不動堂町 8 0 1 番地 オムロン株式会社内
【氏名】 安藤 丹一

【発明者】
【住所又は居所】 京都府京都市下京区塩小路通堀川東入南不動堂町 8 0 1 番地 オムロン株式会社内
【氏名】 竹内 寿

【特許出願人】
【識別番号】 000002945
【氏名又は名称】 オムロン株式会社

【代理人】
【識別番号】 100080034
【弁理士】
【氏名又は名称】 原 謙三
【電話番号】 06-6351-4384

【手数料の表示】
【予納台帳番号】 003229
【納付金額】 21,000円

【提出物件の目録】
【物件名】 特許請求の範囲 1
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 0101830

【書類名】特許請求の範囲**【請求項 1】**

情報送受信装置を携帯した利用者の所定領域に対する出入りを監視し、所定領域に対する警戒動作の制御を行う情報処理装置であって、

複数の上記情報送受信装置それぞれと通信を行う通信装置と、

上記複数の情報送受信装置それぞれの位置を示す位置情報を取得する位置認識装置と、

上記位置情報の所定期間の履歴である位置履歴情報を記憶する履歴記憶装置と、

上記位置情報に基づき、上記情報送受信装置のそれぞれが所定領域内にあるか否かを判定する位置判定手段と、

上記位置判定手段の判定結果に応じて、警戒状態の設定または解除を指示する第 1 警戒指示手段と、

上記情報送受信装置から警戒状態の設定または解除を指示する要求情報を上記通信装置を介して受信し、警戒状態の設定または解除を指示する第 2 警戒指示手段と、

上記位置履歴情報に基づいて、上記第 1 警戒指示手段による指示、および第 2 警戒指示手段による指示のうちいずれかの指示を選択する警戒状態選択手段とを備えていることを特徴とする情報処理装置。

【請求項 2】

上記所定領域内への人の出入りを検知する人行動監視手段をさらに備え、

上記警戒状態選択手段が、上記位置履歴情報に加えて、上記人行動監視手段による検知結果に基づいて指示の選択を行うことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】

上記警戒状態選択手段は、上記位置履歴情報に基づき、上記所定領域内に所定期間存在する情報送受信装置と、所定領域内から所定領域外に移動する情報送受信装置とがあると判定した場合、上記第 1 警戒指示手段の指示を選択し、

上記位置履歴情報に基づき、上記所定領域内に所定期間存在する情報送受信装置と、所定領域外から所定領域内に移動する情報送受信装置とがあると判定した場合、上記第 2 警戒指示手段の指示を選択することを特徴とする請求項 2 に記載の情報処理装置。

【請求項 4】

上記警戒状態選択手段が、情報送受信装置に対して、該情報送受信装置の利用者による入力応答を要求する応答要求手段を備えており、

上記位置履歴情報に基づき、上記所定領域内に情報送受信装置が所定期間ある場合、

上記応答要求手段が上記所定領域内にある情報送受信装置に対して上記入力応答を要求し、

上記入力応答の返信がない場合に、

上記警戒状態選択手段は、上記所定領域内に所定期間存在する情報送受信装置と、所定領域内から所定領域外に移動する情報送受信装置とがあると判定した場合、上記第 1 警戒状態手段の指示を選択し、

上記位置履歴情報に基づき、上記所定領域内に所定期間存在する情報送受信装置と、所定領域外から所定領域内に移動する情報送受信装置とがあると判定した場合、上記第 2 警戒指示手段の指示を選択することを特徴とする請求項 2 に記載の情報処理装置。

【請求項 5】

上記警戒状態選択手段によって選択された上記指示に関する情報を、上記複数の情報送受信装置それぞれに対して上記通信装置を介して通知する警戒状態通知手段をさらに備えていることを特徴とする請求項 1～4 に記載の情報処理装置。

【請求項 6】

上記請求項 1～5 に記載の情報処理装置と、当該情報処理装置と通信をする情報送受信装置とを備える情報処理制御システム。

【請求項 7】

情報送受信装置を携帯した利用者の所定領域に対する出入りを監視し、所定領域に対する警戒動作の制御を行う情報処理装置の制御方法であって、

複数の上記情報送受信装置それぞれと通信を行う通信ステップと、
上記複数の情報送受信装置それぞれの位置を示す位置情報を取得する位置認識ステップ
と、

上記位置情報の所定期間の履歴である位置履歴情報を記憶する履歴記憶ステップと、

上記位置情報に基づき、上記情報送受信装置のそれぞれが所定領域内にあるか否かを判定する位置判定ステップと、

上記位置判定手段の判定結果に応じて、警戒状態の設定または解除を指示する第 1 警戒指示ステップと、

上記情報送受信装置から警戒状態の設定または解除を指示する要求情報を上記通信装置を介して受信し、警戒状態の設定または解除を指示する第 2 警戒指示ステップと、

上記位置履歴情報に基づいて、上記第 1 警戒指示ステップによる指示、および第 2 警戒指示ステップによる指示のうちいずれかを選択する警戒状態選択ステップとを含むことを特徴とする情報処理装置の制御方法。

【請求項 8】

請求項 1～5 の何れか 1 項に記載の情報処理装置を動作させるための制御プログラムであって、コンピュータを上記各手段として機能させるための情報処理装置の制御プログラム。

【請求項 9】

請求項 8 に記載の情報処理装置の制御プログラムが記録されたコンピュータの読取り可能な記録媒体。

【書類名】明細書

【発明の名称】情報処理装置、情報処理制御システム、情報処理装置の制御方法、情報処理装置の制御プログラム、情報処理装置の制御プログラムを記録した記録媒体

【技術分野】

【0001】

本発明は、情報送受信装置を携帯した人が所定領域内から所定領域外に移動する場合に警戒状態とし、該情報送受信装置を携帯した人が所定領域外から所定領域内に移動した場合に警戒状態を解除する情報処理装置に関するものである。

【背景技術】

【0002】

近年、車上荒らしや住居への不法侵入等の様々な犯罪が多発化しており、人々の防犯意識が高まっている。そして、この防犯意識の高まりを受け、様々な防犯用商品が開発されている。

【0003】

例えば、電波を利用した車両用のセキュリティ機構制御システムの一態様として、車両のドア錠の解錠／施錠を行うセキュリティ機構制御システムがある。このセキュリティ機構制御システムでは、ユーザが携帯器を持ち歩くだけで自動的に解錠／施錠が行われ、施錠されていることを容易にこの利用者が確認できるものである（例えば特許文献1～3参照）。このセキュリティ機構制御システムでは、携帯器が信号を送出し、親機がこの信号を受信するようになっており、ユーザがこの携帯器を所持し、車両に近づくだけで自動的に解錠され、逆に車両から離れると施錠されるように構成されている。

【特許文献1】特開2003-27790号公報（公開日2003年1月29日）

【特許文献2】特開2003-27791号公報（公開日2003年1月29日）

【特許文献3】特開2003-301638号公報（公開日2003年10月24日）

【発明の開示】

【発明が解決しようとする課題】

【0004】

ところで、従来のように携帯器を持った利用者の乗降に応じて、自動的に車両のドア錠の解錠／施錠を行うシステムにおいて、セキュリティ管理対象が車両のように複数のユーザによって利用されるものである場合、この携帯器を複数用意しそれぞれを利用可能とする制御システムが考えられる。

【0005】

ところが、複数の携帯器を利用可能とした場合、複数ある携帯器のうちいずれかを車内に置き忘れる可能性が高くなる。このように、複数ある携帯器のうち車内に置き忘れられた携帯器がある場合、従来の構成では次の問題が生じる。

【0006】

つまり、置き忘れた携帯器が車内にあるため、親機が、この携帯器の所有者であるユーザが車内にいると判断し、車両を警戒状態に自動設定しない場合がある。この場合は、携帯器を車内に置き忘れたことにユーザが気付かないまま、車を非警戒状態のままにしてしまうという問題が生じる。

【0007】

また、複数のユーザいずれもが携帯器を所持しており、その複数ユーザのいずれかの降車に応じて、自動的に車両の施錠が行われるように設定される場合、あるいは、車に対して直接、ユーザが施錠をするように指示する場合がある。

【0008】

この両者のいずれの場合であっても、車内に置き忘れられた携帯器がある場合、ユーザ以外の人がこの車に接近すると、自動的に解錠されてしまうという問題が生じる。これは、上記車に対して近づく人がおり、かつ親機の近くに携帯器があるという条件を満たすために、上記車に設定した施錠状態が自動的に解錠されてしまうからである。

【0009】

また、複数の携帯器が利用可能なシステムの場合、ある人は携帯器をもって親機から離れていくがある人は、親機近辺に在るといった状態も起こり得る。

【0010】

この場合、前者の人は、自動的に車に施錠がされたと認識しているが、後者の人が親機のそばに在るため施錠されないこととなる。すなわち、各ユーザの挙動に左右され、一方では施錠する条件を満たしているにもかかわらず、他方では解錠する条件を満たしており、上記の場合は、親機が解錠する条件を選択した結果である。

【0011】

したがって、複数の携帯器が利用可能な場合にはユーザが所望する状態に親機が必ずしも設定しないという問題が生じる。

【0012】

上記特許文献 1～3 での構成では、親機の近辺に置き忘れられた携帯器またはユーザが所持している携帯器が存在する場合、親機の近辺に在る携帯器が置き忘れられた携帯器であるのか、ユーザが所持している携帯機であるのかを区別する手段と、この区別した結果に応じてユーザに適切に通知する手段とがないため、上記した問題には対処することができないこととなる。

【0013】

したがって、携帯器を複数利用可能とした場合、上記特許文献 1～3 の構成では、ユーザが知らない間に、ユーザの意図に反して車に施錠がされない、または施錠した状態から解除されるといふ問題が生じる。

【0014】

本発明は、上記の問題点に鑑みてなされたものであり、その目的は、複数の情報送受信装置が情報処理装置に登録されている場合、当該複数の情報送受信装置の置き忘れによって生じる警戒状態の設定の誤操作を解消することを実現することにある。

【課題を解決するための手段】

【0015】

本発明に係る情報処理装置は、上記課題を解決するために、情報送受信装置を携帯した利用者の所定領域に対する出入りを監視し、所定領域に対する警戒動作の制御を行う情報処理装置であって、複数の上記情報送受信装置それぞれと通信を行う通信装置と、上記複数の情報送受信装置それぞれの位置を示す位置情報を取得する位置認識装置と、上記位置情報の所定期間の履歴である位置履歴情報を記憶する履歴記憶装置と、上記位置情報に基づき、上記情報送受信装置のそれぞれが所定領域内に在るか否かを判定する位置判定手段と、上記位置判定手段の判定結果に応じて、警戒状態の設定または解除を指示する第 1 警戒指示手段と、上記情報送受信装置から警戒状態の設定または解除を指示する要求情報を上記通信装置を介して受信し、警戒状態の設定または解除を指示する第 2 警戒指示手段と、上記位置履歴情報に基づいて、上記第 1 警戒指示手段による指示、および第 2 警戒指示手段による指示のうちいずれかの指示を選択する警戒状態選択手段とを備えていることを特徴とする。

【0016】

上記警戒状態とは、所定の利用者以外が所定の領域に接近することに対して例えば、警告、威嚇、または施錠などの阻害行為を行うよう設定された状態である。そして、本発明に係る情報処理装置は情報送受信装置を携帯した人が所定領域内に在るか否かに応じてこの警戒状態の設定を切り替えるものであり、また当該情報送受信装置とは通信部によって通信可能になっている。

【0017】

この情報処理装置は、位置認識装置と位置判定手段を備えているため、情報送受信装置それぞれの位置を把握することができ、情報送受信装置それぞれが所定領域内に存在するか否かを判定することができる。

【0018】

また、情報処理装置は、履歴記憶装置を備えているため、各情報送受信装置の動きを知ることができ、情報送受信装置が所定領域内から所定領域外に移動したのか、所定領域外から所定領域内に移動したのか、あるいは所定領域内の一定の位置に留まっているのかを知ることができる。

【0019】

また、情報処理装置は、第1警戒指示手段を備えているため、位置履歴情報、すなわち情報処理装置が所定領域内に存在しているのか否かと、所定領域内に入ってきた、または所定領域内から出ていったものであるのか、所定領域内の一定の位置に留まっているのかというの情報に基づき、自動的に警戒状態または非警戒状態に切り替えるのか、あるいはユーザの入力指示に応じて警戒または非警戒に切り替えるのかを決定することができる。

【0020】

したがって、上記情報処理装置は、例えば、情報送受信装置が所定領域内に置き忘れられた場合、他の情報送受信装置が所定領域内に入ってきた際に自動的に非警戒にするのか、常に警戒にするのか、あるいは、所定領域内に入ってきた情報送受信装置に対して通知を行い、情報送受信装置からの指示に応じて、警戒または非警戒を決定するのか選択することができる。

【0021】

それ故、上記情報処理装置は、各情報送受信装置の位置関係と、所定期間での各情報送受信装置の挙動とによって適切に警戒状態の設定または解除を自動で行うのかあるいは情報送受信装置からの指示に基づき行うのかを決定することができる。

【0022】

また、本発明に係る情報処理装置は、上記構成において、上記所定領域内への人の出入りを検知する人行動監視手段をさらに備え、上記警戒状態選択手段が、上記位置履歴情報に加えて、上記人行動監視手段による検知結果に基づいて指示の選択を行う構成であってもよい。

【0023】

これにより、情報処理装置は、人行動監視手段を備えているため、携帯の位置だけでなく、ユーザの位置および挙動も検知することができる。このため、情報送受信装置を携帯する利用者の位置および挙動を精度良く把握することができる。

【0024】

また、本発明に係る情報処理装置は、上記構成において、上記警戒状態選択手段が、上記位置履歴情報に基づき、上記所定領域内に所定期間存在する情報送信装置と、所定領域内から所定領域外に移動する情報送信装置とがあると判定した場合、上記第1警戒指示手段の指示を選択し、上記位置履歴情報に基づき、上記所定領域内に所定期間存在する情報送信装置と、所定領域外から所定領域内に移動する情報送信装置とがあると判定した場合、上記第2警戒指示手段の指示を選択する構成であってもよい。

【0025】

すなわち、上記情報処理装置は、所定領域に所定期間存在する情報送受信装置がある場合これを利用者によって所持されていない情報送受信装置であると特定することができる。

【0026】

また、所定領域内において所定期間、情報送受信装置が有る場合、他の情報送受信装置が所定領域から出て行くときに、所定領域を警戒状態とすることができる。このため、情報処理装置は、例えば所定領域内に置き忘れられた情報送受信装置が有るために警戒状態とならず、警戒状態が解除された状態のままとなることを防ぐことができる。

【0027】

また、上記情報処理装置は、所定領域に所定期間存在する情報送受信装置がある場合、他方の情報送受信装置が所定領域に入ってくるときに、警戒状態である所定領域の警戒を第2警戒指示手段の指示、すなわちユーザの入力指示に基づき、解除することができる。このため、情報処理装置は、例えば所定領域内に置き忘れられた情報送受信装置が有り、

情報送受信装置を所持しない人が所定領域内に入ってきたため、置き忘れられた情報送受信装置と、情報送受信装置を所持していない人との組み合わせを、携帯を所持する正規のユーザと誤って、警戒状態の解除を行うことを防ぐことができる。

【0028】

本発明に係る情報処理装置は、上記構成において、上記警戒状態選択手段が、上記警戒状態選択手段が、情報送受信装置に対して、該情報送受信装置の利用者による入力応答を要求する応答要求手段を備えており、上記位置履歴情報に基づき、上記所定領域内に情報送受信装置が所定期間ある場合、上記応答要求手段が上記所定領域内にある情報送受信装置に対して上記入力応答を要求し、上記入力応答の返信がない場合に、上記警戒状態選択手段は、上記所定領域内に所定期間存在する情報送受信装置と、所定領域内から所定領域外に移動する情報送受信装置とがあると判定した場合、上記第1警戒状態手段の指示を選択し、上記位置履歴情報に基づき、上記所定領域内に所定期間存在する情報送受信装置と、所定領域外から所定領域内に移動する情報送受信装置とがあると判定した場合、上記第2警戒指示手段の指示を選択する構成であってもよい。

【0029】

すなわち、上記情報処理装置は、所定領域に所定期間存在する情報送受信装置に対して、さらに入力応答を要求することによって、所定領域内にある情報処理装置が利用者によって携帯されている情報送受信装置であるのか否かを精度良く判定することができる。

【0030】

また、この利用者が携帯していない情報送受信装置が所定領域内にあると判定した場合において、他の情報送受信装置が所定領域から出て行くときに、所定領域を警戒状態とすることができる。このため、情報処理装置は、例えば所定領域内に置き忘れられた情報送受信装置が有るために警戒状態とならず、警戒状態が解除された状態のままとなることを防ぐことができる。

【0031】

また、上記情報処理装置は、所定領域に所定期間存在する情報送受信装置がある場合、他方の情報送受信装置が所定領域に入ってくるときに、警戒状態である所定領域の警戒を第2警戒指示手段の指示、すなわち利用者の入力指示に基づき、解除することができる。このため、情報処理装置は、例えば所定領域内に置き忘れられた情報送受信装置が有り、情報送受信装置を所持しない人が所定領域内に入ってきたため、置き忘れられた情報送受信装置と、情報送受信装置を所持していない人との組み合わせを、携帯を所持する正規のユーザと誤って、警戒状態の解除を行うことを防ぐことができる。

【0032】

また、本発明に係る情報処理装置は、上記した構成において、上記警戒状態選択手段によって選択された上記指示に関する情報を、上記複数の情報送受信装置それぞれに対して上記通信装置を介して通知する警戒状態通知手段をさらに備えていてもよい。

【0033】

すなわち、上記情報処理装置は、警戒状態通知手段を備えているため、所定領域内に設定される警戒状態がどの状態であるのかをユーザは知ることができる。

【0034】

したがって、情報処理装置によって設定された警戒状態が適切なものであるのか否かを情報送受信装置を介してユーザは知ることができ、不適切な設定である場合は、ユーザはこの設定を変更するように指示を出すことができる。

【0035】

よって、上記情報処理装置は、ユーザの意思を反映させて警戒状態の設定または解除を設定することができる。

【0036】

また、本発明に係る情報処理制御システムは、上記した情報処理装置と、当該情報処理装置と通信をする情報送受信装置とを備える情報処理制御システムである。

【0037】

また、本発明に係る情報処理装置の制御方法は、情報送受信装置を携帯した利用者の所定領域に対する出入りを監視し、所定領域に対する警戒動作の制御を行う情報処理装置の制御方法であって、複数の上記情報送受信装置それぞれと通信を行う通信ステップと、上記複数の情報送受信装置それぞれの位置を示す位置情報を取得する位置認識ステップと、上記位置情報の所定期間の履歴である位置履歴情報を記憶する履歴記憶ステップと、上記位置情報に基づき、上記情報送受信装置のそれぞれが所定領域内にあるか否かを判定する位置判定ステップと、上記位置判定手段の判定結果に応じて、警戒状態の設定または解除を指示する第1警戒指示ステップと、上記情報送受信装置から警戒状態の設定または解除を指示する要求情報を上記通信装置を介して受信し、警戒状態の設定または解除を指示する第2警戒指示ステップと、上記位置履歴情報に基づいて、上記第1警戒指示ステップによる指示、および第2警戒指示ステップによる指示のうちいずれかを選択する警戒状態選択ステップとを含むことを特徴とする。

【0038】

なお、上記情報処理装置は、コンピュータによって実現してもよく、この場合には、コンピュータを上記各手段として動作させることにより上記情報処理装置をコンピュータにて実現させる情報処理装置の制御プログラムを記録したコンピュータ読取り可能な記録媒体も、本発明の範疇に入る。

【発明の効果】

【0039】

本発明に係る情報処理装置は、以上のように、複数の上記情報送受信装置それぞれと通信を行う通信装置と、上記複数の情報送受信装置それぞれの位置を示す位置情報を取得する位置認識装置と、上記位置情報の所定期間の履歴である位置履歴情報を記憶する履歴記憶装置と、上記位置情報に基づき、上記情報送受信装置のそれぞれが所定領域内にあるか否かを判定する位置判定手段と、上記位置判定手段の判定結果に応じて、警戒状態の設定または解除を指示する第1警戒指示手段と、上記情報送受信装置から警戒状態の設定または解除を指示する要求情報を上記通信装置を介して受信し、警戒状態の設定または解除を指示する第2警戒指示手段と、上記位置履歴情報に基づいて、上記第1警戒指示手段による指示、および第2警戒指示手段による指示のうちいずれかの指示を選択する警戒状態選択手段とを備えている。

【0040】

また、本発明に係る情報処理装置の制御方法は、以上のように、複数の上記情報送受信装置それぞれと通信を行う通信ステップと、上記複数の情報送受信装置それぞれの位置を示す位置情報を取得する位置認識ステップと、上記位置情報の所定期間の履歴である位置履歴情報を記憶する履歴記憶ステップと、上記位置情報に基づき、上記情報送受信装置のそれぞれが所定領域内にあるか否かを判定する位置判定ステップと、上記位置判定手段の判定結果に応じて、警戒状態の設定または解除を指示する第1警戒指示ステップと、上記情報送受信装置から警戒状態の設定または解除を指示する要求情報を上記通信装置を介して受信し、警戒状態の設定または解除を指示する第2警戒指示ステップと、上記位置履歴情報に基づいて、上記第1警戒指示ステップによる指示、および第2警戒指示ステップによる指示のうちいずれかを選択する警戒状態選択ステップとを含んでいる。

【0041】

このため、上記情報処理装置は、各情報送受信装置の位置関係と、所定期間での各情報送受信装置の挙動とによって適切に警戒状態の設定または解除を自動で行うのかあるいは情報送受信装置からの指示に基づき行うのかを決定することができるという効果を奏する。

【発明を実施するための最良の形態】

【0042】

本実施の形態に係るカーセキュリティシステム1は、セキュリティ装置2と、このセキュリティ装置2に登録されたセキュリティコントローラ3a~3cとによって構成されるシステムである。そしてこのシステム1は、正規ユーザ以外の人警戒状態に設定されて

いる車のドアを開閉するなどの異常状態に対し、威嚇を行う防犯システムである。

【0043】

なお、車に対する上記異常状態は、例えば、正規ユーザ以外の人が車のトランクを開けようとする行為、フロントガラス等の破壊行為、ジャッキアップなどによって車のタイヤを取り外そうとする行為に伴う振動等として検知される。

【0044】

具体的には、図2および図3に示すように本実施の形態に係るセキュリティシステム1では、セキュリティ装置2が所定の範囲にわたるセキュリティ管理領域50という領域を設定している。図2は、セキュリティ管理領域50における、セキュリティコントローラ3を携帯した人（ユーザ）と、セキュリティコントローラ3を携帯しない人との関係を示す図である。図3は、セキュリティ管理対象である車51を含むセキュリティ管理領域50における、セキュリティコントローラ3を携帯した人（ユーザ）と、セキュリティコントローラ3を携帯しない人との関係を示す図である。

【0045】

このセキュリティ管理領域50とは、当該領域への人の出入りが制限され不正に領域内の管理対象物を利用されないように管理された領域である。例えば、駐車中の車、家屋、敷地、ビル、オフィス、店舗、作業場所、作業機などのセキュリティ管理対象に対して、不正利用や不正侵入等が行われることを防ぐことが求められる領域である。

【0046】

具体的には、図3に示すように、このセキュリティシステム1では、セキュリティコントローラ3を所持するユーザが、このセキュリティ管理領域50内からセキュリティ管理領域50外に出て行くと警戒状態に自動的に設定される。一方、セキュリティシステム1では、上記ユーザがセキュリティ管理領域50外からセキュリティ管理対象である車51に近づくことと警戒設定が自動的に解除されるように設定されている。

【0047】

なお、本明細書においてオートセキュリティ機能とは、セキュリティコントローラ3を保持した正規ユーザが、車51から降車し上記セキュリティ管理領域50外に移動すると自動的に車に警戒状態の設定を行い、逆にセキュリティ管理領域50内にこのユーザが入ると自動的に車に設定されている警戒状態の設定を解除する機能のこととする。

【0048】

また、上記セキュリティ管理領域50の範囲としては、警戒設定対象である車を中心に半径5メートル以内であることが好ましいがこれに限定されるものではない。セキュリティ装置2は、繁華街等、人の往来が激しい地域では、上記した半径5メートルの範囲よりも狭い範囲に上記セキュリティ管理領域50が設定可能となる構成であることが好ましい。

【0049】

また、車に対するこの警戒状態の設定および解除は、正規のユーザが直接所持するセキュリティコントローラ3a～3cによってセキュリティ装置2に指示を出すことで設定を切り替えることもできる。

【0050】

次に、上記したセキュリティシステム1の概略構成について図4を参照して説明する。

【0051】

本実施の形態に係るセキュリティシステム1は、車に搭載されるセキュリティ装置2と、このセキュリティ装置1に対して通信可能となるように登録された3つのセキュリティコントローラ3a～3cを備えている。そして、このセキュリティ装置2とセキュリティコントローラ3a～3cとは、無線によって相互に通信可能となっている。また、セキュリティコントローラ3a～3c同士も互いに無線によって通信可能となっている。

【0052】

なお、本明細書において特にセキュリティコントローラ3a～3cを区別する必要がない場合には、セキュリティコントローラ3と表記する。

【0053】

次に、本実施の形態に係るセキュリティ装置2の概略構成について図1を参照して説明する。図1は、セキュリティ装置2の概略構成の一例を示すブロック図である。

【0054】

本実施の形態に係るセキュリティ装置2は、ACC検出部6、接近物検出部7、通信部4、威嚇部5、異常検出部8、記憶部11、およびセキュリティ管理処理部10を備えている。そして、セキュリティ装置2は、車内のアクセサリ電源（以下ACCと称する）とACC検出部6を介して接続されている。

【0055】

このACC検出部6は、セキュリティ装置2が接続されているACCの電源供給が「オン」または「オフ」であるのかを検出するものである。すなわち、車が停車しキーがはずされるとACCの電源は「オン」から「オフ」に切り換わる。このため、ACC検出部6がACCの電源が「オフ」であると検出した場合、車のエンジンが切られ車は停止状態にあることを示す。逆に、ACC電源検出部6がACCの電源が「オン」であると検出した場合、車が始動中であることを示す。

【0056】

このACC検出部6は、検出したACC電源の「オン」または「オフ」の情報をセキュリティ管理処理部10に送信する。

【0057】

接近物検出部7は、セキュリティシステム1のセキュリティ管理対象である車に接近してくる、例えば人などの対象物を検出するものである。この接近物検出部7は、マイクロ波を利用したドップラー効果によって車両周辺の移動物を検知する、いわゆるドップラセンサによって実現できる。この接近物検出部7は、車に接近する対象物、すなわち上記セキュリティ管理領域50内に侵入する人を検出するとその情報をセキュリティ管理処理部10に送信する。

【0058】

異常検出部8は、セキュリティシステム1のセキュリティ管理対象である車に対して、この車の外部から与えられた振動等の異常を検出するものである。この異常とは、例えば、正規のユーザ以外の人が車のドアを開けようとし生じる振動や、車のガラスの破壊によって生じる振動、車を移動させるためにジャッキアップされることによって生じる車の傾きなどである。異常検出部8は、上記異常を検出した場合、この検出した情報を威嚇部5に通知する。

【0059】

通信部4は、セキュリティ管理処理部10の指示に応じて、上記セキュリティコントローラ3a～3cそれぞれと互いに通信を行うものである。この通信部4は、例えばPINGコマンド等の制御信号をセキュリティコントローラ3a～3cそれぞれに送信したり、セキュリティコントローラ3a～3cそれぞれから送信された警戒設定および／または警戒設定解除等を指示するコマンドを受信したりすることができる。なお、後述するが、通信部4は、セキュリティコントローラ3a～3cそれぞれの所在位置を確認するために、当該セキュリティコントローラ3a～3cから送られる電波を受信するように構成されており、受信したこの電波の情報をセキュリティ管理処理部10に送信する。また、セキュリティコントローラ3a～3cからコマンドを受信した場合も同様にセキュリティ管理処理部10に送信する。

【0060】

威嚇部5は、車が警戒（警戒モード）に設定されている際に、上記異常検出部8がセキュリティシステム1のセキュリティ管理対象である車において異常を検出した場合、警報音を発生させたり、発光させたりして車に接近し不法行為を行おうとする正規ユーザ以外の人に対して威嚇を行うものである。

【0061】

なお、異常が検出された場合に、威嚇部5によって威嚇が行われるとともに、例えば携

帯電話通信網などを利用して、異常が検出されたことを示す情報を、警備サービスを提供するセキュリティセンタに通報することが可能となってもよい。

【0062】

上記セキュリティ管理処理部10は、上記したセキュリティ装置2が備える各部材に対する各種制御を行うものである。このセキュリティ管理処理部10の詳細な説明は後述する。

【0063】

記憶部11は、読み書き可能な不揮発性の記憶媒体であり、セキュリティ管理処理部10が各種処理を行うにあたり必要となる情報を記録したり、記録された情報を参照したりするものである。この記憶部11に記録される情報の詳細な説明は後述する。

【0064】

なお、図4に示す各機能ブロックは、通信部4、威嚇部5、ACC検出部6、接近物検出部7、および異常検出部8の各部材とCPU (central processing unit) と、RAM (random access memory) と、ROM (read only memory) とがそれぞれバスを介して接続されており、CPUがROMに記憶されたプログラムをRAMに読み出しプログラムを実行することで実現できる。

【0065】

また、セキュリティ装置2が備える記憶部11は、例えばフラッシュEEPROMなどの不揮発性記憶媒体によって実現可能である。

【0066】

なお、上記では、各機能ブロックが「CPUなどの演算手段がROMやRAMなどの記録媒体に格納されたプログラムコードを実行することで実現される」場合を例にして説明したが、同様の処理を行うハードウェアで実現してもよい。また、処理の一部を行うハードウェアと、当該ハードウェアの制御や残余の処理を行うプログラムコードを実行する上記演算手段とを組み合わせても実現することもできる。さらに、上記各部材のうち、ハードウェアとして説明した部材であっても、処理の一部を行うハードウェアと、当該ハードウェアの制御や残余の処理を行うプログラムコードを実行する上記演算手段とを組み合わせても実現することもできる。なお、上記演算手段は、単体であってもよいし、装置内部のバスや種々の通信路を介して接続された複数の演算手段が共同してプログラムコードを実行してもよい。

【0067】

上記演算手段によって直接実行可能なプログラムコード自体、または、後述する解凍などの処理によってプログラムコードを生成可能なデータとしてのプログラムは、当該プログラム（プログラムコードまたは上記データ）を記録媒体に格納し、当該記録媒体を配付したり、あるいは、上記プログラムを、有線または無線の通信路を介して伝送するための通信装置で送信したりして配付され、上記演算手段で実行される。

【0068】

なお、例えばバスなどの通信路を介して伝送する場合、通信路を構成する各伝送媒体が、プログラムを示す信号列を伝搬し合うことによって、当該通信路を介して、上記プログラムが伝送される。また、信号列を伝送する際、送信装置が、プログラムを示す信号列により搬送波を変調することによって、上記信号列を搬送波に重畳してもよい。この場合、受信装置が搬送波を復調することによって信号列が復元される。一方、上記信号列を伝送する際、送信装置が、デジタルデータ列としての信号列をパケット分割して伝送してもよい。この場合、受信装置は、受信したパケット群を連結して、上記信号列を復元する。また、送信装置が、信号列を送信する際、時分割／周波数分割／符号分割などの方法で、信号列を他の信号列と多重化して伝送してもよい。この場合、受信装置は、多重化された信号列から、個々の信号列を抽出して復元する。いずれの場合であっても、通信路を介してプログラムを伝送できれば、同様の効果が得られる。

【0069】

ここで、プログラムを配付する際の記録媒体は、取外し可能である方が好ましいが、プ

プログラムを配付した後の記録媒体は、取外し可能か否かを問わない。また、上記記録媒体は、プログラムが記憶されていれば、書換え（書き込み）可能か否か、揮発性か否か、記録方法および形状を問わない。記録媒体の一例として、磁気テープやカセットテープなどのテープ、あるいは、フロッピー（登録商標）ディスクやハードディスクなどの磁気ディスク、または、CD-ROMや光磁気ディスク（MO）、ミニディスク（MD）やデジタルビデオディスク（DVD）などのディスクが挙げられる。また、記録媒体は、ICカードや光カードのようなカード、あるいは、マスクROMやEPROM、EEPROMまたはフラッシュROMなどのような半導体メモリであってもよい。あるいは、CPUなどの演算手段内に形成されたメモリであってもよい。

【0070】

なお、上記プログラムコードは、上記各処理の全手順を上記演算手段へ指示するコードであってもよいし、所定の手順で呼び出すことで、上記各処理の一部または全部を実行可能な基本プログラム（例えば、オペレーティングシステムやライブラリなど）が既に存在していれば、当該基本プログラムの呼び出しを上記演算手段へ指示するコードやポインタなどで、上記全手順の一部または全部を置き換えてもよい。

【0071】

また、上記記録媒体にプログラムを格納する際の形式は、例えば、実メモリに配置した状態のように、演算手段がアクセスして実行可能な格納形式であってもよいし、実メモリに配置する前で、演算手段が常時アクセス可能なローカルな記録媒体（例えば、実メモリやハードディスクなど）にインストールした後の格納形式、あるいは、ネットワークや搬送可能な記録媒体などから上記ローカルな記録媒体にインストールする前の格納形式などであってもよい。また、プログラムは、コンパイル後のオブジェクトコードに限るものではなく、ソースコードや、インタプリタまたはコンパイルの途中で生成される中間コードとして格納されていてもよい。いずれの場合であっても、圧縮された情報の解凍、符号化された情報の復号、インタプリタ、コンパイル、リンク、または、実メモリへの配置などの処理、あるいは、各処理の組み合わせによって、上記演算手段が実行可能な形式に変換可能であれば、プログラムを記録媒体に格納する際の形式に拘わらず、同様の効果を得ることができる。

【0072】

（セキュリティ管理処理部の構成）

次に、セキュリティ管理処理部10の概略構成について説明する。

【0073】

セキュリティ管理処理部10は、図1に示すように機能ブロックとして、ACC判定部21、距離判定部22、接近物解析部23、異常判定部24、セキュリティモード変更部25、置き忘れ判定部26、手動変更判定部20およびセキュリティモード変更判定部27を備えている。

【0074】

手動変更判定部20は、通信部4を介してセキュリティコントローラ3から送信された指示に応じて警戒モードの設定または解除を決定するものである。

【0075】

手動変更判定部20は、決定した結果をセキュリティモード変更部25に送信する。

【0076】

ACC判定部21は、ACC検出部6によって検出されたACC電源のON、OFFの情報を判定するものである。ACC判定部21は、この判定結果をセキュリティモード変更判定部27に送信する。

【0077】

距離判定部22は、通信部4を介して受信したセキュリティコントローラ3a～3cから受信した電波の強度に基づき、セキュリティコントローラ3a～3cのそれぞれの位置を確認するものである。この距離判定部22は、通信部4に対し、応答電波の送信要求を行う制御コマンド（電波要求コマンド）を、各セキュリティコントローラ3a～3cに送

信するように指示する。なお、この電波要求コマンドとは、セキュリティコントローラ 3 に対して、電波をセキュリティ装置 2 に送信するように指示するコマンドであり、例えば PING コマンドなどによって実現できる。

【0078】

すなわち、距離判定部 22 からの指示に応じて、通信部 4 がシステムコントローラ 3 に対して電波を送信するように電波要求コマンドを送信する。一方、セキュリティコントローラ 3 は、このコマンドに応じて、電波を通信部 4 に向けて送信する。

【0079】

通信部 4 は受信したこの電波を距離判定部 12 に渡す。そして、距離判定部 22 は、通信部 4 を介して受信したセキュリティコントローラ 3 の電波強度から、セキュリティ装置 2 から各セキュリティコントローラ 3 までの距離を検出する。すなわち、より正確には距離判定部 22 は、これらセキュリティコントローラ 3a~3c がセキュリティ管理領域 50 内にあるか否か、セキュリティコントローラ 3a~3c のいずれかが一定の場所に留まっているかなどを解析する。この解析は所定時間間隔で行われ、距離判定部 22 は、解析した結果を記憶部 11 にセキュリティコントローラ監視テーブルとして記録する。

【0080】

接近物解析部 23 は、接近物検出部 7 の検出結果に基づき、セキュリティ管理対象である車に接近する人がいるか否かを判定するものである。セキュリティモード変更判定部 27 からの指示に応じて、この接近物解析部 23 は、接近物検出部 7 にセキュリティ管理対象の車に接近する人等を検出するように指示を出す。なお、接近物検出部 7 と接近物解析部 23 とによって、人行動監視手段は実現される。

【0081】

異常判定部 24 は、異常検出部 8 からの検出結果に基づき、セキュリティ管理対象の車に異常状態が生じているか否かを判定するものである。異常判定部 24 は、判定した結果、セキュリティ管理対象である車に異常が生じている場合は、威嚇部 5 に警戒音を発生させるように指示を出す。

【0082】

セキュリティモード変更判定部 27 は、セキュリティ管理対象の車に対するセキュリティモードの変更の有無を判定するものである。セキュリティモード変更判定部 27 は、このセキュリティモードの変更の有無を、距離判定部 22 および接近物解析部 23 の判定結果に基づき、モード設定情報 31 を参照して決定する。このモード設定情報 31 の詳細は後述する。

【0083】

また、セキュリティモードとは、警戒モード、非警戒モード、警戒待ち（警戒準備）モードという 3 つのモードであって、これらもモードが、本実施の形態に係るセキュリティ装置 2 において定義されている。

【0084】

上記警戒モードとは、セキュリティ管理対象の車に正規のユーザ以外がセキュリティ管理領域 50 内に侵入した場合、威嚇部 5 が警戒音等を発生して威嚇するように設定されたモードである。また、非警戒モードとは、正規ユーザのみならず、いかなる人がセキュリティ管理領域 50 内に侵入しても威嚇等行われることがない、上記警戒モードの設定が解除されたモードである。

【0085】

警戒待ち（警戒準備）モードとは、警戒モードと非警戒モードとのモードの移行期間のモードである。このモードにおいて、セキュリティ装置 2 は、距離判定部 22、ACC 判定部 21、接近物解析部 23 から得られる情報等に基づいて、警戒モードから非警戒モードに、あるいは非警戒モードから警戒モードに移行するかを決定する。

【0086】

セキュリティモード変更判定部 27 は、決定したモードへの変更指示を置き忘れ判定部 26 に送信する。

【0087】

置き忘れ判定部26は、セキュリティ管理対象である車にセキュリティコントローラ3a～3cのいずれかが置き忘れていないかを決定するものである。なお、置き忘れ判定の詳細な説明は後述する。

【0088】

置き忘れ判定部26は、車内にセキュリティコントローラ3a～3cのいずれかが置き忘れられているか否かの判定と、セキュリティモード変更判定部27から送信された上記モードの設定指示とに基づき、セキュリティモード変更部25にモードの切替えを指示する。

【0089】

また、置き忘れ判定部26は、車内にセキュリティコントローラ3a～3cのいずれかの置き忘れがあると判定した場合、置き忘れがある旨の通知を、通信部4を介して全てのセキュリティコントローラ3に対して通知する。

【0090】

セキュリティモード変更部25は、置き忘れ判定部26からの指示またはユーザのセキュリティコントローラ3による指示に応じて、セキュリティ装置2の上記モードを切替えるものである。具体的には、セキュリティモード変更部25は、威嚇部5を警戒設定にしたり、威嚇部5を非警戒モードにしたりする。なお、セキュリティモード変更部25はい各部5に指示を出す最終的に設定されるモードをモード設定情報31として記憶部11に記憶する。

【0091】

なお、威嚇部5は、警戒モードの設定がなされている場合のみ、異常判定部24から異常の通知を受けて威嚇を行う。したがって、警戒設定が解除されている際に、異常判定部24から異常の通知を受信したとしても威嚇部5は威嚇を行うことはない。

【0092】

次に、記憶装置11に記録されているセキュリティコントローラ監視テーブル30およびモード設定情報31について説明する。

【0093】

セキュリティコントローラ監視テーブル30は、図5に示すようにセキュリティコントローラ3a～3cそれぞれの電波強度を時系列に記録したテーブルである。このテーブルは、距離判定部22が通信部4を介して各セキュリティコントローラ3a～3cから受信した電波強度を一定の間隔で記録する。図5は、本実施の形態に係るセキュリティ監視テーブル30の一例を示す図である。

【0094】

ところで、本実施の形態に係るセキュリティ装置2では、あらかじめ、セキュリティ管理領域50とそれ以外の領域との境界位置からセキュリティ装置2までの間における、セキュリティコントローラ3の電波強度（基準電波強度と称する）について記憶されている。従って、セキュリティ装置2は、このセキュリティコントローラ監視テーブル30を参照することで、どのセキュリティコントローラ3がセキュリティ管理領域50内にあるか否かについて調べることができる。また、現在と過去における各セキュリティコントローラ3の電波強度を記録しているため、セキュリティ装置2は、現在と過去の両者の電波強度を調べることで、セキュリティコントローラ3がセキュリティ管理対象の車から遠ざかっているのか、近づいているのかについて知ることもできる。

【0095】

さらに予め、セキュリティ管理対象の車の内と外（ユーザが車の乗降口に降り立った位置）とにおける電波強度について記憶されている。このことによって、セキュリティ管理領域50内にある場合であっても車の内にセキュリティコントローラ3があるのか、車の外にあるのか判定することができる。

【0096】

なお、セキュリティコントローラ3a～3cそれぞれの特定は、予め各コントローラ3

のIDがセキュリティ装置2に記録されており、このIDによって受信した電波強度がどのセキュリティコントローラ3から送信されたものであるかを決定することができる。

【0097】

本実施の形態に係るセキュリティコントローラ管理テーブル30は、現在の電波強度とその所定時間前の電波強度の2つを記録しているが、この2つに限定されるものではなく、2より多い時間間隔で測定した電波強度を記録してもよい。この場合は、より細かい電波強度の経時的な変化をすることができるためセキュリティコントローラの位置や移動の有無の検知精度が上がる。

【0098】

また、セキュリティ装置2において距離判定部22は、過去測定された電波強度のうち直前の電波強度のみを記録するように設定し、距離判定部22が通信部4を介して取得した現在の各セキュリティコントローラ3の電波強度と、この管理テーブル30に記録された電波強度とを比較する構成であってもよい。この場合は、過去に測定された電波強度のうち、直近の電波強度のみを記録しておくだけでよい。使用記録領域のメモリを最低限に抑えることができる。

【0099】

また、本実施の形態に係るセキュリティ装置2では各セキュリティコントローラ3のIDを予め記憶することで、セキュリティ装置2は、各セキュリティコントローラ3を特定する構成であった。しかし、予め各セキュリティコントローラ3に使用される電波の周波数を異ならせ、各セキュリティコントローラ3を特定する構成であってもよい。さらには、各セキュリティコントローラ3からセキュリティ装置2に対して送信する電波の送信タイミングを所定の時間だけずらすように設定することで、各セキュリティコントローラ3を特定する構成であってもよい。

【0100】

モード設定情報31は、現在セキュリティ装置2において設定されているセキュリティモードを示す情報である。すなわち、このモード設定情報31は、セキュリティモード変更部25が威嚇部5に対してモードの設定を指示するとともに、この指示したモードの設定について記録する。

【0101】

(セキュリティコントローラの構成)

次に、図6を参照してセキュリティコントローラ3の構成について説明する。図6は、セキュリティコントローラ3の概略構成の一例を示すブロック図である。

【0102】

セキュリティコントローラ3は、コマンド入力部40、通信部41、通知部42、コントローラ制御部43、および識別情報記憶部44を備えている。

【0103】

コマンド入力部40は、ユーザが入力操作等を行うためのものである。ユーザによって入力された情報はコントローラ制御部43に送信される。

【0104】

通信部41は、他のセキュリティコントローラ3や、セキュリティ装置2との通信を行うものである。通信部41は、他のセキュリティコントローラ3またはセキュリティ装置2に対して制御コマンド等を送信する。また、セキュリティコントローラ3は、セキュリティ装置2からPINGコマンドを受信するとこのコマンドをコントローラ制御部43に送信する。そしてコントローラ制御部43は、コマンドを解釈し通信部41に当該セキュリティ装置2に電波を送信するように指示を出す。この指示に応じて通信部41は電波をセキュリティ装置2に対して送信する。

【0105】

通知部42は、セキュリティ装置42または他のセキュリティコントローラ3から送信されたコマンドの内容をユーザに対して通知するものである。通知部42は、例えば液晶ディスプレイなどの表示装置や、音声マイク等によって実現できる。

【0106】

コントローラ制御部43は、上記したコマンド入力部40、通信部41、および通知部42の各部材の各種制御を行うものである。

【0107】

識別情報記録部44は、通信先である他のセキュリティコントローラ3およびセキュリティ装置2とを特定するための情報であって、自装置、自装置以外のセキュリティコントローラ3、およびセキュリティ装置2のID情報である。

【0108】

なお、上記したセキュリティコントローラ3の機能ブロックは、上記コマンド入力部40、通信部41、および通知部42の各部材がバスを介してCPU、ROM、およびRAMと接続されており、CPUがROMに記録されたプログラムをRAMに読み出し実行することで実現できるし、各機能を実現するICを備えることによっても実現できる。

【0109】

(警戒設定待ち処理)

次に、本実施の形態に係るセキュリティ装置2における非警戒の状態(非警戒モード)から警戒状態(警戒モード)に移行する処理、すなわち警戒待ち処理の一例について説明する。なお、図7は、本実施の形態に係るセキュリティ装置2における警戒待ち処理の一例を示すフローチャートである。

【0110】

まず、セキュリティ装置2は車のACC電源が「オン」から「オフ」に切り換わったか否かを判定する(ステップS10、これ以降においてはS10のように称する)。すなわち、セキュリティ装置2では、ACC判定部21が、ACCの電源が「オン」から「オフ」に切り換わるか否かを監視しており、ACCの電源が「オフ」へと切り換わらない限り(S10において「No」の場合)、非警戒モードのままである。

【0111】

そして、ステップS10において「Yes」の場合、すなわち、ユーザが車のエンジンのキーを回し電源を切ってACC電源が「オン」から「オフ」に切り換わると、セキュリティ装置2は、ACCの電源が「オフ」になってから10分以上経過したか否かを判定する(S11)。

【0112】

つまり、本実施の形態に係るセキュリティ装置2では、10分以上経過する間に、警戒モードに移行するための条件が満たされない場合は、非警戒モードのままとする設定となっている。

【0113】

ここまでの処理において10分以上経過していない場合(ステップS11において「No」)、次にセキュリティ装置2は、セキュリティコントローラ3a~3cが、セキュリティ管理領域50外に出たか否かを判定する(S12)。すなわち、セキュリティ装置2において、距離判定部22が、各セキュリティコントローラ3a~3cから受信した電波強度をセキュリティコントローラ監視テーブル30に記録している。そして、予め記憶されている基準電波強度と、現在受信しているセキュリティコントローラ3a~3cの電波強度とを比較し、現在受信している上記電波強度が、基準電波強度よりも大きい小さいかを調べることによってこの判定ができる。

【0114】

つまり、セキュリティコントローラ監視テーブル30に記録されているセキュリティコントローラ3の電波強度の履歴と、現在の受信しているセキュリティコントローラ3の電波強度それぞれとを比較し、セキュリティコントローラ3のそれぞれの電波強度が基準電波強度よりも大きい状態から小さい状態に変化した場合、このセキュリティコントローラ3はセキュリティ管理領域50外に出たと判定できる。

【0115】

ステップS10~ステップS12までの処理経過時間内に、セキュリティコントローラ

3がセキュリティ管理領域50外に出ていない場合(S12において「No」)、セキュリティ装置2はセキュリティコントローラ3a~3cのいずれかから警戒モードへの変更を指示するコマンドが送信されたか否かを判定する(S13)。

【0116】

一方、セキュリティコントローラ3がセキュリティ管理領域50外に出ている場合(S12において「Yes」)は、車内に置き忘れたセキュリティコントローラ3があるか否かを判例する(S17)。

【0117】

なお通常、ステップS10~ステップS12までの処理経過時間は非常に短時間である。このため、最初にセキュリティ装置2がステップS12の判定を行う場合はACCの電源が「オフ」になったばかりで、セキュリティコントローラ3a~3cのいずれもセキュリティ管理領域50内にある可能性が高い。したがって、最初にセキュリティ装置2がステップS12の判定を行う場合は、通常は次のステップS13に進むこととなる。

【0118】

そこで、次に、セキュリティ装置2は、ステップS13においてユーザの指示に応じて、セキュリティコントローラ3a~3cのいずれかから警戒モードに変更するよう指示するコマンドが送信されたか否かを判定する。

【0119】

そして、セキュリティ装置2がセキュリティコントローラ3a~3cのいずれかから警戒モードに変更するよう指示するコマンドを受信していないと判定した場合(ステップS13において「No」)は、ステップS11に戻る。また、ステップ13において「Yes」の場合は、置き忘れのセキュリティコントローラ3があるか否かを判定する(S14)。

【0120】

すなわち、セキュリティ装置2では、ユーザから直接警戒モードへの変更指示が送信される、あるいはセキュリティコントローラ3がセキュリティ管理領域50外にでるまで、ステップS11~S13を繰り返す。そして、このステップS11~S13の判定処理の間に、ACCの電源が「オフ」になってから10分以上経過した場合は、警戒設定を行わない(S11「Yes」)ように構成されている。

【0121】

次に、ステップS13の判定において、セキュリティ装置2が、セキュリティコントローラ3a~3cのいずれかから警戒モードへの変更指示を示すコマンドを、受信した場合、セキュリティコントローラ3a~3cのうち車内に置き忘れられたものがあるか否かを判定する(S14)。この判定において、セキュリティ装置2がセキュリティコントローラ3a~3cのうち車内に置き忘れられたものがあると判定した場合(S14において「Yes」)、セキュリティコントローラ3の置き忘れをユーザに通知する(S15)。一方、セキュリティ装置2が、置き忘れのセキュリティコントローラ3がないと判定した場合(S14において「No」)は、警戒モードに設定を変更する(S16)。

【0122】

また、ステップS17において車内に置き忘れたセキュリティコントローラ3があるか否かを判定した結果(S17)、上記置き忘れたセキュリティコントローラ3がある場合は、ステップS15に進む。一方、車内に置き忘れたセキュリティコントローラ3がない場合はステップS16に進む。これ以降の処理は上記にて説明したため省略する。

【0123】

なお、セキュリティ装置2におけるセキュリティコントローラ3の置き忘れの判定および、セキュリティコントローラ3の置き忘れがある場合のユーザへの通知方法の詳細は後述する。

【0124】

以上が本実施形態に係るセキュリティ装置2における処理フローの一例である。ここで、セキュリティコントローラ3についての置き忘れ判定がない構成の場合の警戒設定待ち

処理を比較例として図8を参照して説明する。図8は、本実施の形態に係るセキュリティ装置2の比較例における警戒待ち処理の一例を示すフローチャートである。

【0125】

比較例の処理ステップでは、ステップS110～ステップS113までの処理フローは、上記した処理フローのステップS10～ステップS13までの処理と同じであるため、説明は省略する。

【0126】

この比較例では、ステップ112において、セキュリティコントローラ3がセキュリティ管理領域50外に出た場合、セキュリティ装置2は警戒モードへの設定変更を行う。あるいはステップS113において、セキュリティコントローラ3から警戒モードへの変更指示を示すコマンドが送信される場合、セキュリティ装置2は警戒モードへの設定変更を行う。したがって、これら2点が比較例では本実施の形態に係るセキュリティ装置2の処理フローとは異なることとなる。

【0127】

つまり、本実施形態に係るセキュリティ装置2では、警戒モードに設定変更する直前の処理において置き忘れたセキュリティコントローラ3の有無の判定を行い、セキュリティコントローラ3の置き忘れがある場合は、それを通知できる。

【0128】

したがって、車内にセキュリティコントローラ3が置き忘れられた場合、ユーザにこの置き忘れられたセキュリティコントローラ3があることをユーザに通知することができる。また、セキュリティ装置2は、上記通知を行った後に、セキュリティ管理対象の車51を警戒状態に設定する構成である。

【0129】

つまり、セキュリティ装置2は、置き忘れられたセキュリティコントローラ3が車内にある場合、ユーザにセキュリティコントローラ3の置き忘れに対する注意を促した上で車を警戒モードの設定に切り替えることができる。

【0130】

また、置き忘れられたセキュリティコントローラ3が車内にあるため、セキュリティ装置2が、ユーザがまだ車内にいる状態ととらえ非警戒状態のままとすることを防ぐ構成でもある。したがって、セキュリティ装置2は、セキュリティコントローラ3a～3cいずれかを置き忘れた場合であっても、非警戒モードのままにして正規ユーザ以外の人の接近を許し被害に遭うことを防止することができる。

【0131】

一方、比較例では、セキュリティコントローラ3から警戒モードへの設定指示を示すコマンドを受信したり、セキュリティコントローラ3がセキュリティ管理領域50外に移動したりすると警戒モードに設定される構成である。

【0132】

このため、この比較例は、本実施の形態に係るセキュリティ装置2と同様にセキュリティコントローラ3a～3cいずれかを置き忘れた場合であっても、非警戒モードのままにして正規ユーザ以外の人の接近を許し被害に遭うことを防止することができる。

【0133】

しかし、警戒モードに設定された後、セキュリティコントローラ3がセキュリティ装置2の近くに置き忘れられているため、ユーザ以外の人が車に接近するだけで警戒モードを解除してしまうということが、ユーザが知らない間に発生することとなる。

【0134】

(警戒処理および警戒解除処理)

次は逆に警戒モードに設定されている状態から、この警戒状態を解除するまでの警戒処理について図9を参照して説明する。図9は、本実施の形態に係るセキュリティ装置2における警戒処理および警戒処理解除の一例を示すフローチャートである。

【0135】

まず、前提としてセキュリティ管理対象である車において警戒モードが設定されている状況からこの処理の説明を行うものとする。

【0136】

セキュリティ装置2は、警戒モードに設定されている間、セキュリティコントローラ3 a~3 cのいずれかから警戒モードの解除指示を示すコマンドが送信されたか否かを判定する(S20)。

【0137】

セキュリティ装置2は、セキュリティコントローラ3 a~3 cの何れからも警戒モードの解除指示を示すコマンドを受信していない場合(S20においてNo)、セキュリティ管理対象である車に異常が生じているか否かを判定する(S21)。

【0138】

一方、セキュリティ装置2が、セキュリティコントローラ3 a~3 cの何れから警戒モードの解除指示を示すコマンドを受信した場合(S20においてYes)は、設定されている警戒モードを解除して非警戒モードとする。

【0139】

すなわち、通信部4を介してセキュリティコントローラ3から受信した警戒モードの解除指示を示すコマンドを、通信部4を介してセキュリティモード変更部25が受信する。そしてセキュリティモード変更部25は、この受信したコマンドに応じて威嚇部5に対して警戒モードの設定を解除するように指示を出すとともに、モード設定情報31を警戒モードから非警戒モードに書き換える。

【0140】

つまり、本実施形態に係るセキュリティ装置2では、ユーザが、所持しているセキュリティコントローラ3から警戒モードの設定の解除指示を行う場合、警戒解除を即座に行える構成となっている。

【0141】

ステップS21において、セキュリティ装置2が、セキュリティ管理対象の車に異常が生じていないと判定した場合(S21において「Yes」)、人の接近の有無を判定する(S22)。一方、ステップS21において、セキュリティ装置2がセキュリティ管理対象である車に異常が生じたと判定した場合、異常が発生したことをセキュリティコントローラ3 a~3 cに通知し(S26)、威嚇を行う(S27)。そして、セキュリティ装置2は、しばらく威嚇を行った後、再度に警戒状態に戻る。

【0142】

すなわち、異常検出部8を介して、異常判定部24がセキュリティ管理対象の車に異常が生じていると判定した場合、異常の発生を、通信部4を介してセキュリティコントローラ3 a~3 cに通知するとともに、威嚇部5にも威嚇動作を行うように指示を出す。威嚇部5は、セキュリティモード変更部25によって警戒モードに設定されているため、異常判定部24から威嚇動作の指示を受けると、警報音を発生させたり、発光させたりする。

【0143】

ステップS22において、セキュリティ装置2が人の接近を検知した場合(S22において「Yes」)は、セキュリティ装置2の近くにセキュリティコントローラ3 a~3 cの何れかがあるか否かを判定する(S23)。

【0144】

一方、セキュリティ装置2が、人の接近を検知しない場合(S22において「No」)、ステップS20に戻る。すなわち、S20~S22の間の検知を繰り返すこととなる。

【0145】

次に、ステップS23の判定において、セキュリティ装置2が自装置の近くにセキュリティコントローラ3 a~3 cの何れかがあると判定した場合(S23)、すなわちセキュリティ管理領域50内にセキュリティコントローラ3 a~3 cの何れかがあると判定した場合、セキュリティコントローラ3 a~3 cの何れかのうち置き忘れられたものがあるか否かを判定する(S24)。

【0146】

一方、近くにセキュリティコントローラ3a~3cの何れかが無いと判定した場合は、ステップS20に戻る。

【0147】

すなわち、セキュリティ装置2は、人の接近を検知し（S22において「Yes」）、かつセキュリティ管理領域50内にセキュリティコントローラ3a~3cの何れかが存在する（S23において「No」）まで、セキュリティコントローラ3からの警戒モードの設定解除指示があるか否か（S20）、セキュリティ管理対象の車に異常が生じたか否か（S21）を繰り返し判定する構成である。

【0148】

ステップS23において、セキュリティ装置2が自装置の近く、すなわちセキュリティ管理領域50内にセキュリティコントローラ3a~3cの何れかが存在すると判定した場合（S23において「Yes」）、セキュリティコントローラ3a~3cの何れかのうち置き忘れられたものがあるか否かを判定する（S24）。

【0149】

置き忘れられたセキュリティコントローラ3があると判定した場合（S24において「Yes」）は、再度ステップ20からの処理を繰り返す。

【0150】

一方、置き忘れられたセキュリティコントローラ3がないと判定した場合（S24において「No」）、警戒解除を行う（S25）。

【0151】

すなわち、置き忘れられたセキュリティコントローラ3があると判定した場合、置き忘れられたセキュリティコントローラ3と正規のユーザ以外の接近という組み合わせがあるため、セキュリティ装置2は警戒モードを解除しない。このため、セキュリティ装置2では、正規ユーザは、セキュリティコントローラ3からセキュリティ装置2に対して警戒モードの設定解除を指示するコマンドを送信することで警戒モードを解除する必要がある。

【0152】

このようにして、本実施形態に係るセキュリティ装置2は、セキュリティコントローラ3a~3cの何れかが置き忘れられた場合であっても、この置き忘れられたセキュリティコントローラ3a~3cのいずれかと、人との接近という組み合わせで警戒モードの設定を誤って解除することを防ぐことができる。

【0153】

以上が本実施形態に係るセキュリティ装置2における警戒処理および警戒解除処理の一例である。ここで、セキュリティコントローラ3の置き忘れ判定がない構成の場合の処理フローを比較例として図10を参照して説明する。図10は、本実施の形態に係るセキュリティ装置2の比較例における警戒処理および警戒解除処理の一例を示すフローチャートである。

【0154】

比較例の処理ステップでは、ステップS120~ステップS123、ステップS125~ステップS126までの処理フローは、上記した処理フローのステップS20~ステップS23、ステップS25~ステップS26までの処理と同じであるため、説明は省略する。

【0155】

この比較例では、ステップ123において、セキュリティ装置2が、セキュリティ管理領域50内にセキュリティコントローラ3a~3cのいずれかが存在する場合、警戒解除を行う（S124）点が本実施の形態に係るセキュリティ装置2の処理フローとは異なることとなる。

【0156】

したがって、この比較例では、車内に置き忘れられたセキュリティコントローラ3があつた場合、正規ユーザ以外がセキュリティ管理対象の車に接近したときでも、警戒モードの

設定を誤って解除することとなる。

【0157】

このため、本実施の形態に係るセキュリティ装置2では、置き忘れられたセキュリティコントローラ3と正規ユーザ以外の人の接近との組み合わせの場合は、警戒モードの設定を解除しない構成であるため、比較例の構成と比べてより好ましい構成であると言える。

【0158】

(置き忘れ判定処理)

次に置き忘れ判定処理について詳細に説明する。

【0159】

本実施の形態に係るセキュリティ装置2では、警戒モードへの設定条件が揃った場合、もしくはセキュリティコントローラ3a~3cの何れかから警戒モードへの設定指示のコマンドを受信した場合、セキュリティ管理領域50内にあるセキュリティコントローラ3に対して警戒モードへの設定変更する旨の通知を行う。

【0160】

なお、この通知は、セキュリティコントローラ3の通知部42が通知内容を表示することによって行われてもよいし、通知部42が音声によって通知内容をユーザに通知する構成であってもよい。また、セキュリティコントローラ3の通知部42がバイブレーション機能を有しており、振動によって通知する構成であってもよい。さらには表示と音声と振動とのうちのいずれかの組み合わせによってユーザに通知するものであってもよい。

【0161】

このように通知することによって正規のユーザが携帯するセキュリティコントローラ3であれば、この通知に対する応答が返されることとなる。しかし、置き忘れられたセキュリティコントローラ3の場合は、この通知に対する応答がないこととなる。

【0162】

したがって、セキュリティ装置2は、この通知に対して反応の無いセキュリティコントローラ3を置き忘れられたものと判定する。

【0163】

より具体的に言えば、まずセキュリティモード変更判定部27が、ACC判定部21および距離判定部22からの情報を受信すると、警戒モードへの設定変更の判定を行い、設定を変更する場合には警戒モードとなるように置き忘れ判定部26に指示を出す。

【0164】

すなわち、セキュリティモード変更判定部27は、ACC判定部21からACCの電源が「オン」から「オフ」に切り換わったという情報と、距離判定部22から、セキュリティコントローラ3a~3cの何れかがセキュリティ管理領域50内からセキュリティ管理領域50外に出たという情報とを受信した場合、警戒モードへの設定変更指示の情報を置き忘れ判定部26に送信する。

【0165】

置き忘れ判定部26は、セキュリティモード変更判定部27からの上記情報を受信すると、セキュリティコントローラ監視テーブル30を参照して、セキュリティ管理領域50内にあるセキュリティコントローラ3を特定する。

【0166】

そして、置き忘れ判定部26は、特定した上記セキュリティコントローラ3に対して通信部4を介して応答を要求するコマンド(応答要求コマンド)を送信する。置き忘れ判定部26は、所定期間(例えば5分間)待って、通知先のセキュリティコントローラ3から応答コマンドに対する返答が来ない場合は、このセキュリティコントローラ3は置き忘れられたものであると判定する。

【0167】

また、この応答要求コマンドに対する返答として、警戒モードへの設定変更を要求するコマンドをセキュリティコントローラ3a~3cの何れかから受信した時点で、セキュリティ管理領域50内にあるセキュリティコントローラ3を置き忘れとする構成であってもよい。

よい。

【0168】

また、上記応答要求コマンドに対して最初に応答してきたセキュリティコントローラ 3 以外のセキュリティ管理領域 50 内にあるセキュリティコントローラ 3 を置き忘れられたものとして判定する構成でもよい。この場合は、セキュリティ装置 2 は、セキュリティ領域内にあるセキュリティコントローラ 3 のうち唯 1 つに対してオートセキュリティ機能可能とすることで、確実にユーザが携帯しているセキュリティコントローラ 3 のみをオートセキュリティ機能に対して有効とすることができる。

【0169】

従って、この場合は置き忘れられたセキュリティリモコンを含むセキュリティ管理領域 50 内にあるセキュリティコントローラ 3 において、特定のセキュリティコントローラ 3 以外はオートセキュリティ機能を有効としないことで誤って警戒モードが解除される可能性を低減させることができる。

【0170】

このように、本実施の形態に係るセキュリティ装置 2 は上記したように、セキュリティ管理領域 50 内にあるセキュリティコントローラ 3 に対して応答要求コマンドを送信する、そして、この応答要求コマンドに対する返答の状態によって、セキュリティ管理領域 50 内にあるセキュリティコントローラ 3 に対して置き忘れか否かを判定する構成である。

【0171】

このため、例えば、正規ユーザが車の洗車などをおこなっており、セキュリティ管理領域 50 内に存在する場合であっても、応答要求コマンドに対する返答として警戒モードの設定を行わないように促す内容を通知することで、誤って警戒モードに設定されることを防ぐことができる。

【0172】

さらに、本実施形態に係るセキュリティ装置 2 において、上記セキュリティコントローラ 3 の置き忘れ判定を以下のように行う構成とすることもできる。

【0173】

すなわち、セキュリティコントローラ 3 a ~ 3 c の何れかから警戒モードへの設定指示を示すコマンドを受信した場合、所定期間（例えば 5 分間）経過した後、セキュリティ管理領域 50 内にセキュリティコントローラ 3 a ~ 3 c の何れかがある場合は、このセキュリティ管理領域 50 内のセキュリティコントローラ 3 を置き忘れられたものと判定する構成であってもよい。

【0174】

あるいは、上記したようにセキュリティモード変更判定部 27 が警戒モードへの設定変更の条件を満たすと判定した場合、所定期間（例えば 5 分間）経過した後、セキュリティ管理領域 50 内にセキュリティコントローラ 3 a ~ 3 c の何れかがある場合は、このセキュリティ管理領域 50 内のセキュリティコントローラ 3 を置き忘れられたものと判定する構成であってもよい。

【0175】

また、上記所定期間を例えば 30 分間というように、ある程度長い期間に設定し、この間においてセキュリティ管理領域 50 内に留まっているセキュリティコントローラ 3 があれば、これを置き忘れられたものとみなしてもよい。この場合は、セキュリティ管理領域 50 内にあるセキュリティコントローラ 3 の動向をより精度良く観察した上で置き忘れられたものか否かを判定できる。

【0176】

つまり、セキュリティモード変更判定部 27 が、通信部 4 を介してセキュリティコントローラ 3 a ~ 3 c のいずれかから警戒モードへの設定変更指示を受信する、あるいは、ACC 判定部 21 および距離判定部 22 から送信された情報に基づき、警戒モードに設定を変更すると判定すると、置き忘れ判定部 26 に警戒モードへの設定変更指示を送信する。

【0177】

そして、置き忘れ判定部 26 は、セキュリティモード変更判定部 27 からの指示を受信すると、所定時間経過後にセキュリティコントロール監視テーブル 30 を参照して、セキュリティ管理領域 50 内にあるセキュリティコントローラ 3 を置き忘れであると特定する。

【0178】

また、セキュリティモード変更判定部 27 が警戒モードへの設定変更の条件を満たすと判定した場合、セキュリティ管理領域 50 内にあるセキュリティコントローラ 3 を置き忘れられたものと判定する構成であってもよい。

【0179】

これらの場合は、置き忘れ判定部 26 がセキュリティコントローラ監視テーブル 30 の情報のみを参照して置き忘れを判定できる。このため、上記したセキュリティ管理領域 50 内にあるセキュリティコントローラ 3 に応答を要求する構成よりもより簡単な構成でセキュリティコントローラ 3 の置き忘れに関する判定ができる。

【0180】

しかし、複数ユーザのうち一部のユーザが車内に残ってセキュリティコントローラ 3 を保持している場合も、このセキュリティコントローラ 3 を置き忘れとするため、置き忘れか否かの判定精度の点では、本実施形態に係るセキュリティ装置 2 の構成の方が好ましい。

【0181】

また、上記置き忘れ判定部 3 の置き忘れ判定の精度を高めるために、セキュリティコントローラ 3 とセキュリティ装置 2 は以下の構成をさらに備えていてもよい。

【0182】

すなわち、セキュリティコントローラ 3 は、例えば加速度センサまたは振動センサ（不図示）をさらに備え、ユーザの携帯によってセキュリティコントローラ 3 に生じる振動等の動きをセキュリティ装置 2 に伝えることができる。

【0183】

一方、セキュリティ装置 2 は、上記セキュリティコントローラ 3 から送信される振動等の動きの情報を検出する振動検出部（不図示）と、この検出結果からセキュリティコントローラ 3 に動きがあるか否かを判定する振動判定部（不図示）とをさらに備えた構成としてもよい。

【0184】

この場合は、セキュリティ装置 2 は、ユーザによって携帯されることによってセキュリティコントローラ 3 に生じる振動を検知することができる。したがって、置き忘れ判定部 26 は、セキュリティコントローラ 3 がユーザによって所持されている状態であるのか否かという情報を、さらに上記した置き忘れ判定処理に加えることができることとなる。このため、セキュリティ装置 2 は、セキュリティ管理領域 50 内にあるセキュリティコントローラ 3 が置き忘れられたものであるか否かの判定精度を高めることができる。

【0185】

また、セキュリティ装置 2 は、車内の人の動きを検出する、上記接近物検出部 7 と同様のドップラセンサ（不図示）と、セキュリティ管理処理部 10 にこのドップラセンサからの情報を解析するドップラセンサ解析部（不図示）とをさらに備えた構成としてもよい。

【0186】

あるいは、シートにかかる人の重さを検出するために、車内のシート下に、所定の圧力以上を検出する圧力センサ（不図示）と、セキュリティ管理処理部 10 に、この圧力センサからの情報を解析する圧力センサ解析部（不図示）とをさらに備えた構成であってもよい。そして、これらドップラセンサおよび／または圧力センサによって検知した情報に基づき、ドップラセンサ解析部および／または圧力センサ解析部が車内にユーザがいるか否かを判定する。そして、置き忘れ判定部 26 は、これらドップラセンサ解析部および／または圧力センサ解析部による判定結果を、上記した置き忘れ判定処理を行う情報としてさらに用いる構成としてもよい。この場合は、車内におけるユーザの有無に関する情報をさ

らに置き忘れ判定処理に加えることとなる。

【0187】

このため、置き忘れ判定部26は、セキュリティ管理領域50内にあるセキュリティコントローラ3が置き忘れられたものであるのか否かの判定精度を高めることができる。

【0188】

また、本実施形態に係るセキュリティ装置2は、上記したようにセキュリティ管理領域50内にあるセキュリティコントローラ3に対する監視によって置き忘れを判定するだけでなく、セキュリティコントローラ3の置き忘れに気づいたユーザからの通知に対しても対処できる構成である。

【0189】

すなわち、セキュリティ装置2は、セキュリティ管理領域50外のセキュリティコントローラ3a~3cのいずれから、車内にセキュリティコントローラ3a~3cのいずれかを置き忘れていることを通知する情報を受信した場合、この情報において指定されているセキュリティ管理領域50内のセキュリティコントローラ3を置き忘れられたものとする。

【0190】

なお、セキュリティ管理領域50外からなされるこの通知には、置き忘れたセキュリティコントローラ3のID等識別情報が含まれている。このため、セキュリティ装置2は、セキュリティ管理領域50内にあるセキュリティコントローラ3のうちどれが置き忘れたものであるのか特定することができる。

【0191】

また、セキュリティ装置3a~3cのいずれかがセキュリティ管理領域50内にある場合であっても、警戒設定を指示する要求を予め設定されている場合は、セキュリティ装置2は警戒モードへの設定変更の条件が揃った場合は、セキュリティ管理領域50内にあるセキュリティリモコン3を置き忘れられたものとみなす構成であってもよい。

【0192】

(置き忘れ判定後の通知)

上記にて、「警戒処理および警戒解除処理」に説明したように、セキュリティ装置2が置き忘れられたセキュリティコントローラ3が車内にあると判定した場合、セキュリティ装置2はユーザに置き忘れられたセキュリティコントローラ3がある旨を通知するように構成されている。以下、この通知を行う処理について説明する。

【0193】

すなわち、セキュリティ装置2は、管理対象である車51を警戒モードに設定する際に、置き忘れられたセキュリティコントローラ3があると判定すると、セキュリティコントローラ3a~3cに対して、セキュリティ管理領域50内にセキュリティコントローラ3a~3cのいずれかが置き忘れられていることを通知する。

【0194】

そして、さらに通知したセキュリティコントローラ3以外のセキュリティコントローラ3の状態を表示させるように、セキュリティコントローラ3に情報を送信することが好ましい。これは、通知されたもの以外のセキュリティコントローラ3がセキュリティ管理領域50内にあるか否かという情報を表示させることで、どのセキュリティコントローラ3が置き忘れられているものであり、どのセキュリティコントローラ3がユーザに携帯されたままセキュリティ管理領域50内にあるのかを示すことができる。

【0195】

ところで、本実施の形態に係るセキュリティ装置2では、上記した通知をセキュリティコントローラ3a~3cに行った後、置き忘れ判定部26は、警戒モードへの変更指示を示す情報をセキュリティモード変更部25に送信するとともに、置き忘れられたセキュリティコントローラ3として特定したセキュリティコントローラ3の情報(不図示)を記憶部11に記憶しておく。

【0196】

そして、セキュリティモード変更部 25 は、置き忘れ判定部 26 から受信した情報に基づき、警戒モードに設定するように威嚇部 5 に指示を出す。

【0197】

このようにして、セキュリティ装置 2 は、置き忘れられたセキュリティコントローラ 3 の有無を判定した後に、管理対象である車 51 を警戒モードに設定するのである。

【0198】

また、管理対象である車 51 が警戒モードに設定された後、セキュリティコントローラ 3 を携帯したユーザが管理対象の車 51 に戻ってきた場合、セキュリティ装置 2 は、ユーザが携帯しているセキュリティコントローラ 3 によって警戒モードの解除を行うようにする。すなわち、セキュリティ装置 2 は、オートセキュリティ機能を停止し、ユーザが手動で警戒モードの設定を解除するまでは警戒モードの設定を解除しない構成である。

【0199】

また、セキュリティ装置 2 は、上記のようにオートセキュリティ機能を停止するのではなく、置き忘れられたセキュリティコントローラ 3 があると判定した場合、この置き忘れられたセキュリティコントローラ 3 に対して、電源を切るように指示する構成とすることで、誤って警戒モードの設定を解除することを防ぐこともできる。

【0200】

このように本実施の形態に係るセキュリティ装置 2 では、警戒モードに設定する際に置き忘れ判定部 26 が、セキュリティ管理領域 50 内に置き忘れられたセキュリティコントローラ 3 があるか否かを判定することができる構成である。そして、置き忘れられたセキュリティコントローラ 3 がある場合、この置き忘れられたセキュリティコントローラ 3 が存在することを示す情報をセキュリティコントローラ 3a~3c に通知する構成である。そして、セキュリティ装置 2 は、この通知を行った後に警戒モードに設定を切り替えるように構成されている。

【0201】

すなわち、セキュリティ装置 2 は、置き忘れられたセキュリティコントローラ 3 が、セキュリティ管理領域 50 内にあると判断した場合、このセキュリティコントローラ 3 の存在をユーザに認識させることができる。そして、ユーザに置き忘れられたセキュリティコントローラ 3 の存在を認識させた上で、管理対象である車 51 を警戒モードに切り替えるように構成されている。このようにセキュリティ装置 2 は、セキュリティ管理対象である車 51 が非警戒モードのままの設定とならないように構成されている。

【0202】

したがって、置き忘れられたセキュリティコントローラ 3 がある場合であっても、セキュリティ管理対象である車 51 が非警戒状態のままとならず正規ユーザ以外の人によって被られる被害を防ぐことができる。

【0203】

さらには、セキュリティ装置 2 は、置き忘れられたセキュリティコントローラ 3 がある場合、オートセキュリティ機能による警戒モード設定の解除を行わないように構成されている。このため、セキュリティコントローラ 3 を所持しない人がセキュリティ管理対象である車 51 に接近した場合、セキュリティ装置 2 は、置き忘れられたセキュリティコントローラ 3 と、この接近してきた人との組み合わせによって、誤って警戒モードの設定を自動的に解除することを防ぐことができる。

【0204】

(セキュリティ管理領域 50 内にあるセキュリティコントローラへの通知)

上記にて、置き忘れられたセキュリティコントローラ 3 がある場合、セキュリティ装置 2 は、他のセキュリティコントローラ 3 に「置き忘れられたセキュリティコントローラ 3」の存在を通知する。そして、セキュリティ装置 2 は、置き忘れられたセキュリティコントローラ 3 があることをユーザに認識させるため通知する構成であった。

【0205】

次に、セキュリティコントローラ 3 a ~ 3 c をそれぞれ所持する各ユーザの行動に応じて、セキュリティ装置 2 がさらに適切な通知を行う構成について説明する。

【0206】

本実施形態に係るセキュリティ装置 2 は、上記したように複数のセキュリティコントローラ 3 a ~ 3 c が登録されている。このため、セキュリティコントローラ 3 a ~ 3 c のそれぞれの位置関係に応じて、警戒モードの設定がどのタイミングで行われたかをユーザが把握できる必要がある。

【0207】

ところで、セキュリティ装置 2 は、上記したようにセキュリティコントローラ 3 a ~ 3 c のいずれかがセキュリティ領域内からセキュリティ領域外に移動した場合、オートセキュリティ機能によってセキュリティ管理対象の車 5 1 が警戒モードに設定される構成である。

【0208】

しかし、複数のユーザがそれぞれ車 5 1 から降車して移動するタイミングが異なる場合がある。そこで、どのセキュリティコントローラ 3 がセキュリティ管理領域 5 0 から出た時点で警戒モードに設定するのかを決定する必要がある。

【0209】

本実施の形態に係るセキュリティ装置 2 では、警戒モードへの設定変更指示を出す条件は、ACC 電源が OFF になって所定時間内、すなわち 10 分間内にセキュリティ管理領域 5 0 外に出て行くセキュリティコントローラ 3 がある場合としていた。この条件をより正確に言えば、10 分間内にセキュリティコントローラ 3 a ~ 3 c のいずれか 1 つがセキュリティ管理領域 5 0 外に出て行く場合に警戒モードへの設定変更指示を出す条件である。

【0210】

したがって、セキュリティコントローラ 3 a ~ 3 c それぞれを携帯するユーザが一斉にセキュリティ管理対象である車 5 1 から出て略同時にセキュリティ管理領域 5 0 内に出れば問題がない。また、ばらばらのタイミングで各ユーザがセキュリティ管理領域 5 0 外に出る場合でも、警戒設定を行うか否かを決定する期間、すなわち ACC の電源が「オン」から「オフ」に変わってから 10 分間であれば問題がない。

【0211】

つまり、最初にセキュリティ管理領域 5 0 外に出たユーザのセキュリティコントローラ 3 によって、一旦警戒モードの設定が指示されるが、次のユーザがセキュリティ管理領域 5 0 内にいるため、この次のユーザのセキュリティコントローラ 3 によって警戒モードの解除指示が出され、この次のユーザがセキュリティ管理領域 5 0 外に出た時点で再度警戒モードの設定指示が行われることとなる。

【0212】

したがって、セキュリティ装置 2 は、結果として最後のユーザがセキュリティ管理領域 5 0 外に出た時点で警戒モードの設定指示を行うことができる。

【0213】

しかし、ACC の電源が「オン」から「オフ」に変わってから 10 分間経過する間に、セキュリティコントローラ 3 を有するすべてのユーザがセキュリティ管理領域 5 0 外に出ていない場合は、非警戒状態のままとなる。

【0214】

そこで、本実施の携帯に係るセキュリティ装置 2 は、上記図 7 に示す「警戒設定待ち処理」で説明したように、セキュリティコントローラ 3 がセキュリティ管理領域 5 0 外に出たから所定期間（5 分間）待って、セキュリティコントローラ 3 a ~ 3 c のいずれかにおいて置き忘れられたものがあるか否かの判定を行い、置き忘れられたセキュリティコントローラ 3 が無い場合は、警戒モードに設定を変更指示する構成となっている。

【0215】

すなわち、セキュリティ装置 2 は、10 分の間でセキュリティ管理領域 5 0 外にセキ

リティコントローラ 3 を所持して出た複数のユーザのうち、最後にこのセキュリティ管理領域 50 外を出たユーザの時間から 5 分間経過した後に、置き忘れられたセキュリティコントローラ 3 があるか否かを判定する。

【0216】

したがって、まだ他にもユーザがセキュリティ管理領域 50 内にいる場合であっても、このユーザが所持するセキュリティコントローラ 3 は置き忘れられたものではないため、セキュリティ装置 2 は警戒モードの設定変更指示を行うことができる。ただし、セキュリティ装置 2 は、セキュリティコントローラ 3 の置き忘れ判定が行われた際に、少なくともセキュリティ管理領域 50 内にいるセキュリティコントローラ 3 に対して警戒状態に設定される旨の通知を行う。これは、セキュリティ管理領域 50 内にいるユーザが知らない間に、セキュリティ管理対象である車 51 が警戒モードの設定変更され、意図せぬ威嚇等を受けることを防ぐためである。

【0217】

なお、この通知は、セキュリティ管理領域 50 内にあるセキュリティコントローラ 3 に対する通知のみならず、全てのセキュリティコントローラ 3 に対して行われる設定であってもよい。この場合は、他のセキュリティコントローラ 3 に対しても行うことで、他のユーザは、セキュリティ管理対象である車 51 が警戒状態に設定されたことを確認することができる。

【0218】

ところで、本実施の形態に係るセキュリティ装置 2 は、セキュリティ管理対象である車 51 に置き忘れられたセキュリティコントローラ 3 があると判定した場合、この判定結果に基づく通知を他のセキュリティコントローラ 3 に行った上で、セキュリティ管理対象である車 51 に対して警戒モードの設定を行う構成であった。しかし、セキュリティ装置 2 を、上記通知後、警戒モードの設定を行わない構成としてもよい。

【0219】

すなわち、セキュリティ装置 2 は、セキュリティコントローラ 3 a ~ 3 c に、セキュリティコントローラ 3 a ~ 3 c のいずれかがセキュリティ管理対象である車 51 に置き忘れているということを通知した後、警戒モードに設定を変更しないように構成されていてもよい。ただし、セキュリティ装置 2 は、警戒モードに設定を変更しないということをさらに、セキュリティ装置 3 a ~ 3 c に通知する。

【0220】

このようにして、セキュリティ装置 2 は、セキュリティコントローラ 3 a ~ 3 c のいずれかがセキュリティ管理領域 50 内に置き忘れられているという通知と、警戒モードに設定を変更しないという通知との 2 回の通知を行うことで、ユーザに対応を促すことができる。また、セキュリティコントローラ 3 を置き忘れたユーザが、セキュリティ管理対象である車 51 に戻ってきた時にも警戒モードに設定されていないため予期せず威嚇されることがない。

【0221】

さらにまた、セキュリティ装置 2 は、セキュリティ管理領域 50 内にセキュリティコントローラ 3 があると判定した場合、この判定結果に基づく通知を他のセキュリティコントローラ 3 に行った上で、警戒モードの設定を行わない構成としてもよい。

【0222】

すなわち、セキュリティ装置 2 は、セキュリティコントローラ 3 a ~ 3 c に、セキュリティコントローラ 3 a ~ 3 c のいずれかがセキュリティ管理領域 50 内にあるということを通知した後、警戒モードに設定を変更しないように構成されていてもよい。ただし、セキュリティ装置 2 は、警戒モードに設定を変更しないということをさらに、セキュリティ装置 3 a ~ 3 c に通知する。好ましくは、セキュリティ管理領域 50 内にあるセキュリティコントローラ 3 の情報を示す通知も行う。この通知を行うことで、ユーザはセキュリティ管理領域 50 内にあるセキュリティコントローラ 3 を確認することができ、この確認の上で、警戒モードに設定するあるいは設定しないという指示セキュリティ装置 2 に指示する

ことができる。

【0223】

このようにして、セキュリティ装置2は、セキュリティコントローラ3a~3cのいずれかがセキュリティ管理領域50内にあるという通知と、警戒モードに設定を変更しないという通知との2回の通知を行うことで、ユーザに対応を促すことができる。また、セキュリティコントローラ3を置き忘れたユーザが、セキュリティ管理対象である車51に戻ってきた時にも警戒モードに設定されていないため予期せず威嚇されることがない。また、セキュリティ管理領域50内にいるユーザの知らない間に、セキュリティ管理対象の車51が警戒モードに設定され、このユーザが予期せぬ威嚇を受けることを防ぐことができる。

【0224】

さらにまた、セキュリティ装置2は、セキュリティ管理領域50内にセキュリティコントローラ3があると判定した場合、例えばユーザから警戒モードへの変更指示が出された場合であっても警戒モードの設定を行わない構成としてもよい。

【0225】

ただし、セキュリティ装置2は、警戒モードに設定を変更しないということをさらに、セキュリティ装置3a~3cに通知する。そして、この通知に応じて再度ユーザが警戒モードへの設定変更を指示した場合は、警戒モードに設定を変更する。

【0226】

このように、セキュリティコントローラ3による警戒モードへの設定指示を行えないようにすることで、ユーザにセキュリティ管理領域50内にセキュリティコントローラ3が存在することを知らせることができる。すなわち、通常行えるはずのセキュリティコントローラ3の操作とは異なる挙動をセキュリティ装置2が行うことで、ユーザにセキュリティ管理領域50内にあるセキュリティコントローラ3の存在に気づかせることができるのである。また、セキュリティ管理対象の車51の複数ユーザの全てが同じ場所に居合わせている場合、ユーザは、セキュリティ管理領域50内にあるセキュリティコントローラ3は複数ユーザのうちの何れかが置き忘れたセキュリティコントローラ3であることが分かる。

【0227】

さらにまた、他のセキュリティコントローラ3によって警戒モードに設定指示されている場合、設定解除処理の置き忘れられたセキュリティコントローラ3があるか否かの判定において、例えば30分間以上の長時間セキュリティ管理領域50内にあるセキュリティコントローラ3は全て置き忘れられたセキュリティコントローラ3とするように構成してもよい。

【0228】

すなわち、この場合、長時間セキュリティ管理領域50内に留まっているセキュリティコントローラ3をすべて置き忘れと判定するため、車内においてユーザが所持しているセキュリティコントローラ3も置き忘れられたものとみなすこととなる。

【0229】

従って、セキュリティ管理対象である車51が警戒モードに設定されている場合、例えばセキュリティコントローラ3を所持したまま、車内でユーザが仮眠をしても、このセキュリティコントローラ3を置き忘れとすることができるため、このユーザのセキュリティコントローラ3とセキュリティ管理対象である車51に近づく正規ユーザ以外の人の組み合わせによって、警戒モードを誤って解除することを防ぐことができる。

【0230】

また、本実施の形態に係るセキュリティシステム1では、セキュリティコントローラ3a~3cすべてがオートセキュリティ機能を利用可能とする構成であった。しかし、複数のセキュリティコントローラ3a~3cのうちいずれか1台のみをオートセキュリティ機能を有効とする構成であってもよい。

【0231】

このように、セキュリティコントローラ 3 a ~ 3 c が、セキュリティ装置 2 に登録されている場合であっても、オートセキュリティ機能を有効とするのは、このセキュリティコントローラ 3 a ~ 3 c のうちのいずれか 1 つとすることで、置き忘れられたセキュリティコントローラ 3 によって生じる問題を低減できる。すなわち、置き忘れられたセキュリティコントローラ 3 と正規ユーザ以外の人の接近によって自動的に設定されている警戒モードが解錠される確率を低くすることができる。

【0232】

このオートセキュリティ機能を有効とするセキュリティコントローラ 3 は、例えば、工場出荷時にオートマスタリモコンとして出荷されたセキュリティコントローラ 3 のみとしてもよい。あるいは、セキュリティコントローラ 3 a ~ 3 c のうちユーザによってオートセキュリティ機能を有効とするセキュリティリモコン 3 を設定されたものとしてもよい。

【0233】

前者に比べて後者の方が、セキュリティコントローラ 3 に対して自由にオートセキュリティ機能を有効な装置とすることができるため、設定の自由度が増すこととなる。

【0234】

さらには、オートセキュリティ機能を有効としたいセキュリティコントローラ 3 から他のセキュリティコントローラ 3 に対して通信を介してオートセキュリティ機能を有効としないように指示する形態であってもよい。

【0235】

また、セキュリティ装置 2 からオートセキュリティ機能を有効とするセキュリティコントローラ 3 はどれかという問合せをセキュリティコントローラ 3 a ~ 3 c それぞれに通知し、応答があったセキュリティコントローラ 3 のみをオートセキュリティ機能が有効な装置としてもよい。

【0236】

さらには、ユーザが最初あるいは最後に警戒モードへの設定指示等操作を行ったセキュリティコントローラ 3 をオートセキュリティ機能が有効な装置としてもよい。

【0237】

車 5 1 を駐車した際に最初あるいは最後に管理対象である車 5 1 から離れたセキュリティコントローラ 3 を、オートセキュリティ機能が有効な装置としてもよい。

【0238】

なお、セキュリティコントローラ 3 a ~ 3 c において、いずれか 1 つだけがオートセキュリティ機能を有効とする場合は、どのセキュリティコントローラ 3 が、オートセキュリティ機能を有効とするのかについて、セキュリティコントローラ 3 の通知部 4 2 においてユーザに通知されていることが好ましい。

【0239】

なお、本実施形態に係るセキュリティシステム 1 では、セキュリティコントローラ 3 は、セキュリティコントローラ 3 a ~ 3 c という 3 台であったが、この 3 台に限定されるものではなく、セキュリティ管理対象のユーザの数に応じて必要なだけ設定することができる。

【0240】

また、本実施形態に係るセキュリティシステム 1 では、セキュリティ管理対象が車 5 1 であったが、このセキュリティ管理対象は車 5 1 に限定されるものではなく、例えば家屋、ビル、オフィス、または金庫などであってもよい。ただし、セキュリティ管理対象が家屋、ビル、オフィス、または金庫などの場合、非警戒モードから警戒モードへの設定変更を行うトリガは、ACC 電源の「オン」から「オフ」への切替えではなく、ドアや出入口に備えられた警戒モード設定ボタン等をユーザが押すことで実現できる。

【0241】

また、上記したセキュリティコントローラ 3 は、例えば携帯電話と組み合わせられたものであってもよい。この場合は、セキュリティ装置 2 は、GPS による位置情報を利用できるため、より正確なセキュリティコントローラ 3 の位置を把握することができる。

【産業上の利用可能性】

【0242】

セキュリティ装置 2 は、セキュリティコントローラ 3 を所持しない人の接近または侵入等に対して威嚇行為および通知を行うことができるため、特定の権限を有する人以外の利用を制限することが好ましい領域における監視にも適用できる。

【図面の簡単な説明】

【0243】

【図 1】本発明の実施形態を示すものであり、セキュリティ装置の概略構成の一例を示すブロック図である。

【図 2】セキュリティ管理領域における、セキュリティコントローラ 3 を携帯した人と、セキュリティコントローラを携帯しない人との関係を示す図である。

【図 3】セキュリティ管理対象である車を含むセキュリティ管理領域における、セキュリティコントローラ 3 を携帯した人（ユーザ）と、セキュリティコントローラ 3 を携帯しない人との関係を示す図である。

【図 4】本実施の形態に係るセキュリティシステムの概略構成の一例を示すブロック図である。

【図 5】本実施の形態に係るセキュリティ監視テーブルに記録される情報の一例を示す図である。

【図 6】本実施の形態に係るセキュリティコントローラの概略構成の一例を示すブロック図である。

【図 7】本実施の形態に係るセキュリティ装置における警戒待ち処理の一例を示すフローチャートである。

【図 8】本実施形態の比較例としてのセキュリティ装置における警戒待ち処理の一例を示すフローチャートである。

【図 9】本実施の形態に係るセキュリティ装置における警戒処理および警戒処理解除の一例を示すフローチャートである。

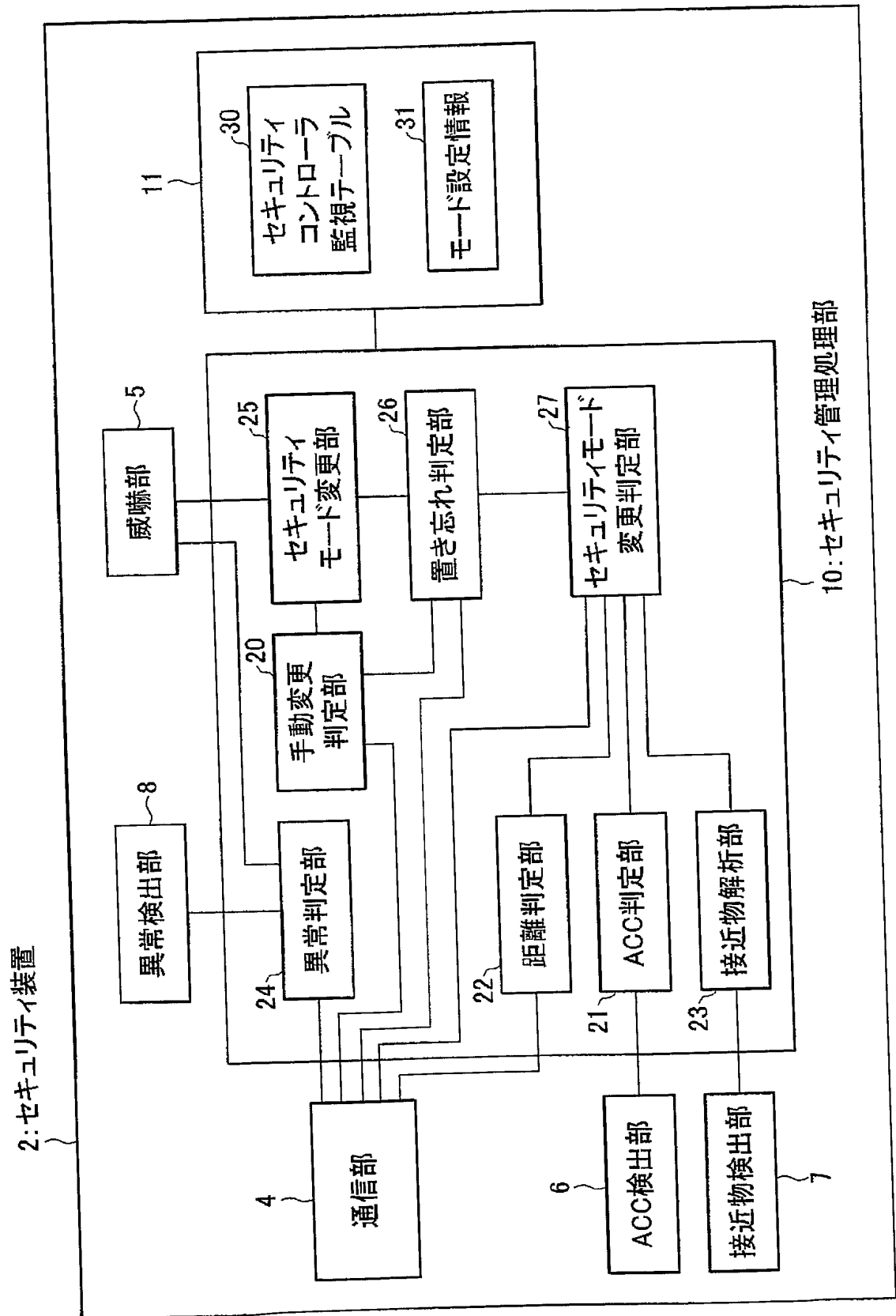
【図 10】本実施形態の比較例としてのセキュリティ装置における警戒処理および警戒処理解除の一例を示すフローチャートである。

【符号の説明】

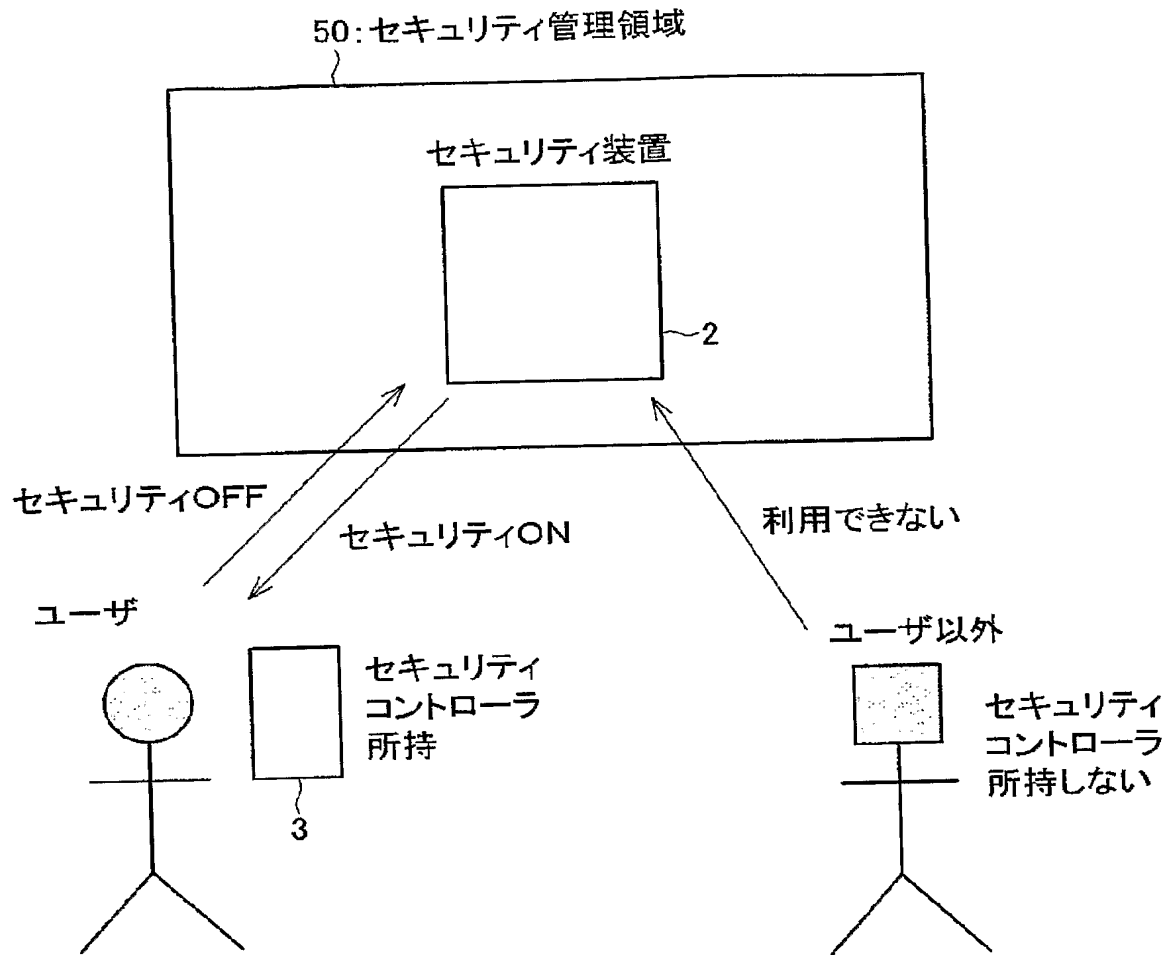
【0244】

- 1 セキュリティシステム（情報処理制御システム）
- 2 セキュリティ装置（情報処理装置）
- 3 セキュリティコントローラ（情報送受信装置）
- 4 通信部（通信装置、位置認識装置）
- 6 異常検出部
- 7 接近物検出部（人行動監視手段）
- 10 セキュリティ管理処理部
- 11 記憶部（履歴記憶装置）
- 20 手動変更判定部（第 2 警戒指示手段）
- 22 距離判定部（位置判定手段）
- 23 接近物解析部（人行動監視手段）
- 24 セキュリティモード変更判定部（第 1 警戒指示手段）
- 26 置き忘れ判定部（警戒状態選択手段、応答要求手段）
- 25 セキュリティモード変更部
- 30 セキュリティコントローラ監視テーブル（位置履歴情報）
- 50 セキュリティ管理領域（所定領域）

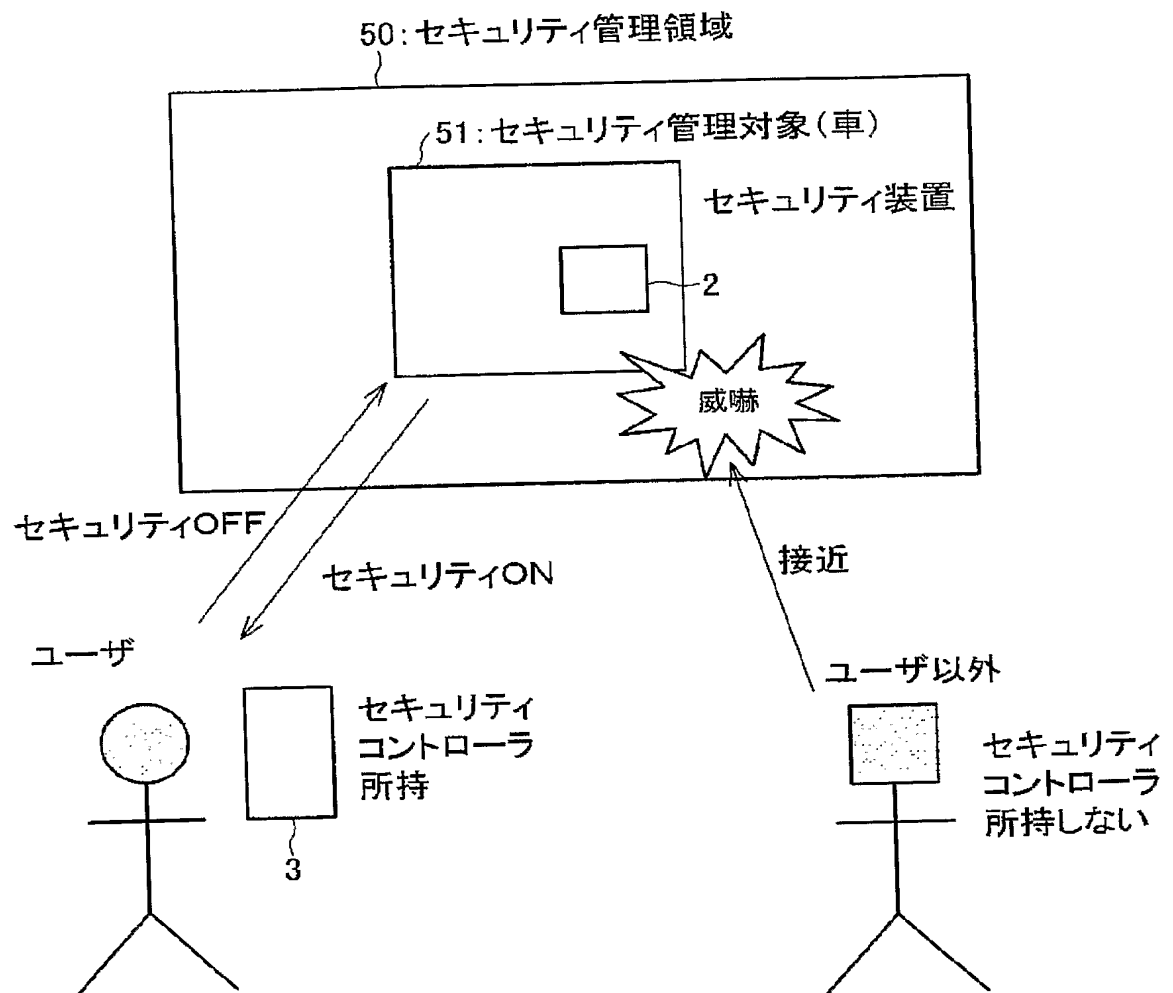
【書類名】 図面
【図 1】



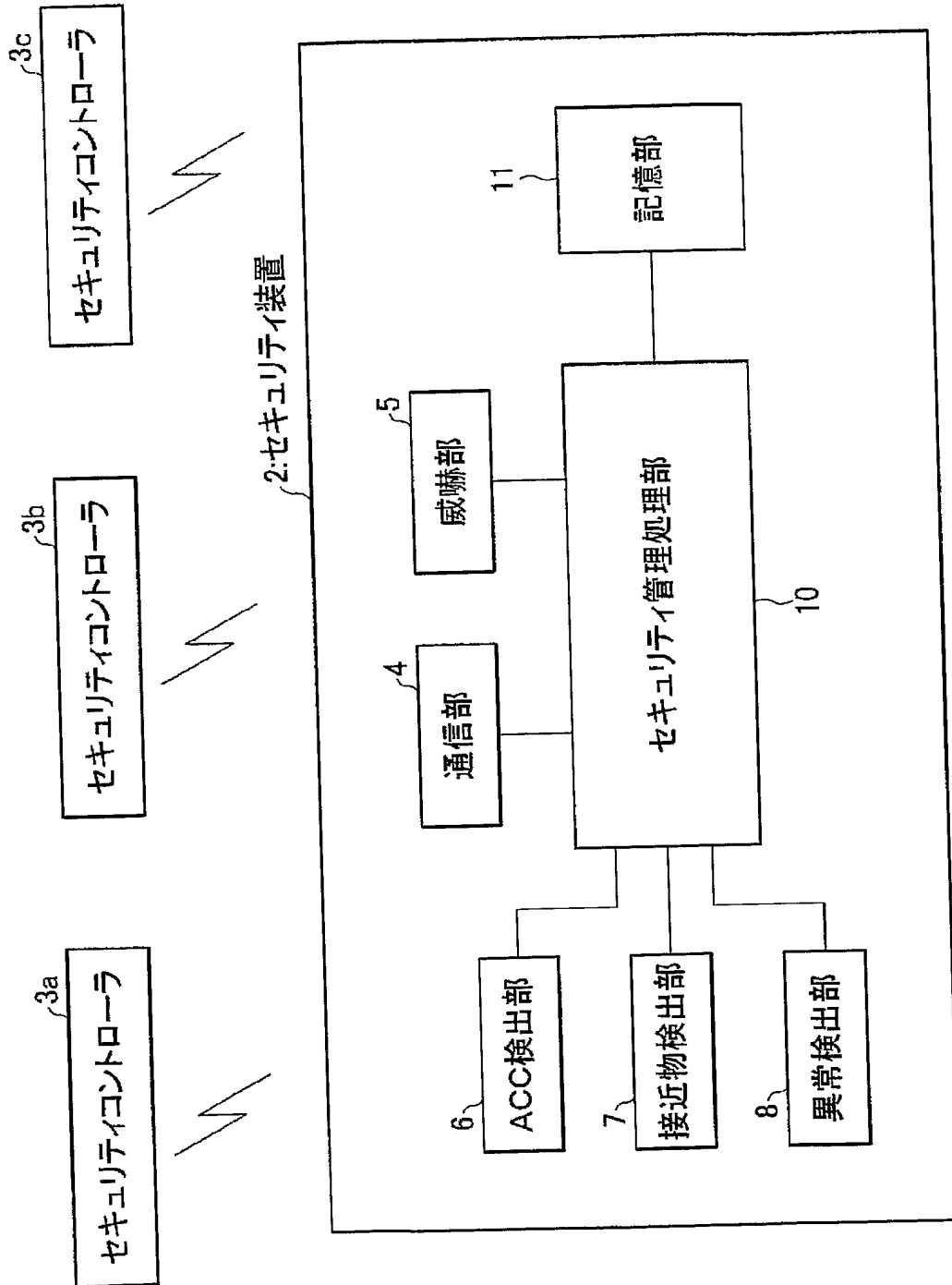
【図 2】



【図 3】



【図 4】

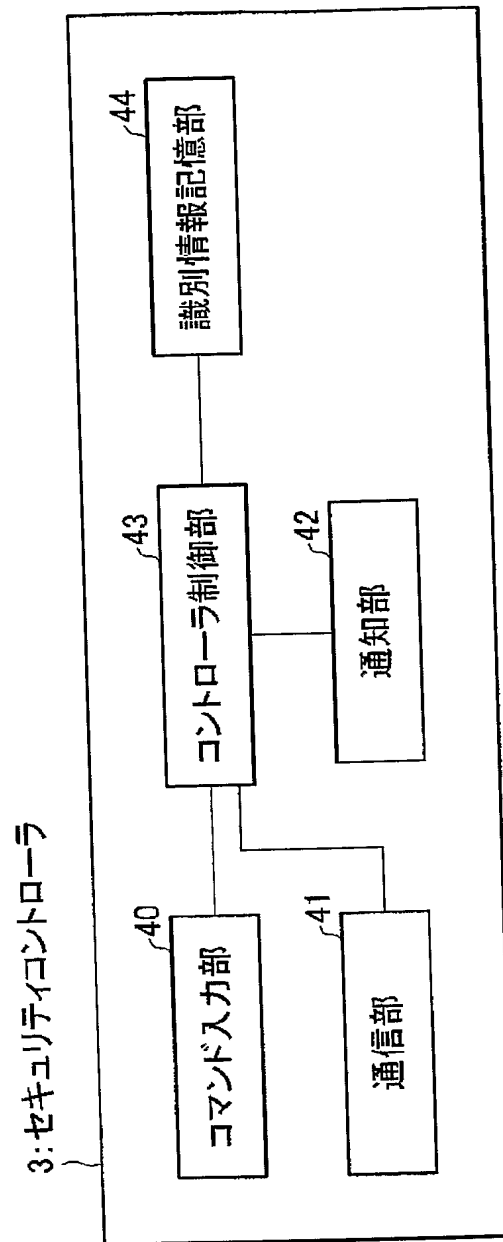


1: セキュリティシステム

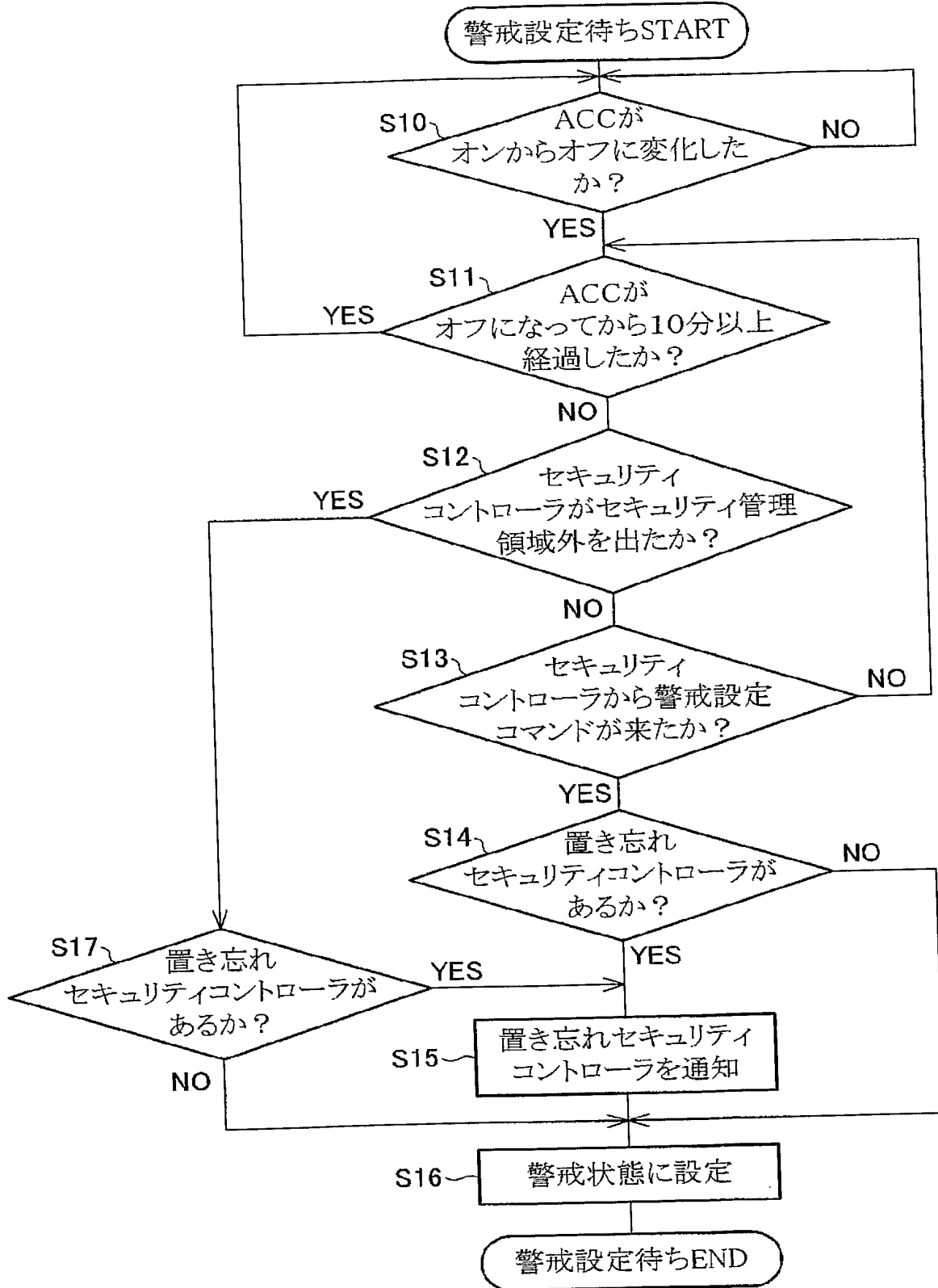
【図 5】

時間 セキュリティ コントローラ	0:00 (現在)	0:20
セキュリティコントローラ3a	電波強度3.5	電波強度2.0
セキュリティコントローラ3b	電波強度3	電波強度2.3
セキュリティコントローラ3c	電波強度10	電波強度10

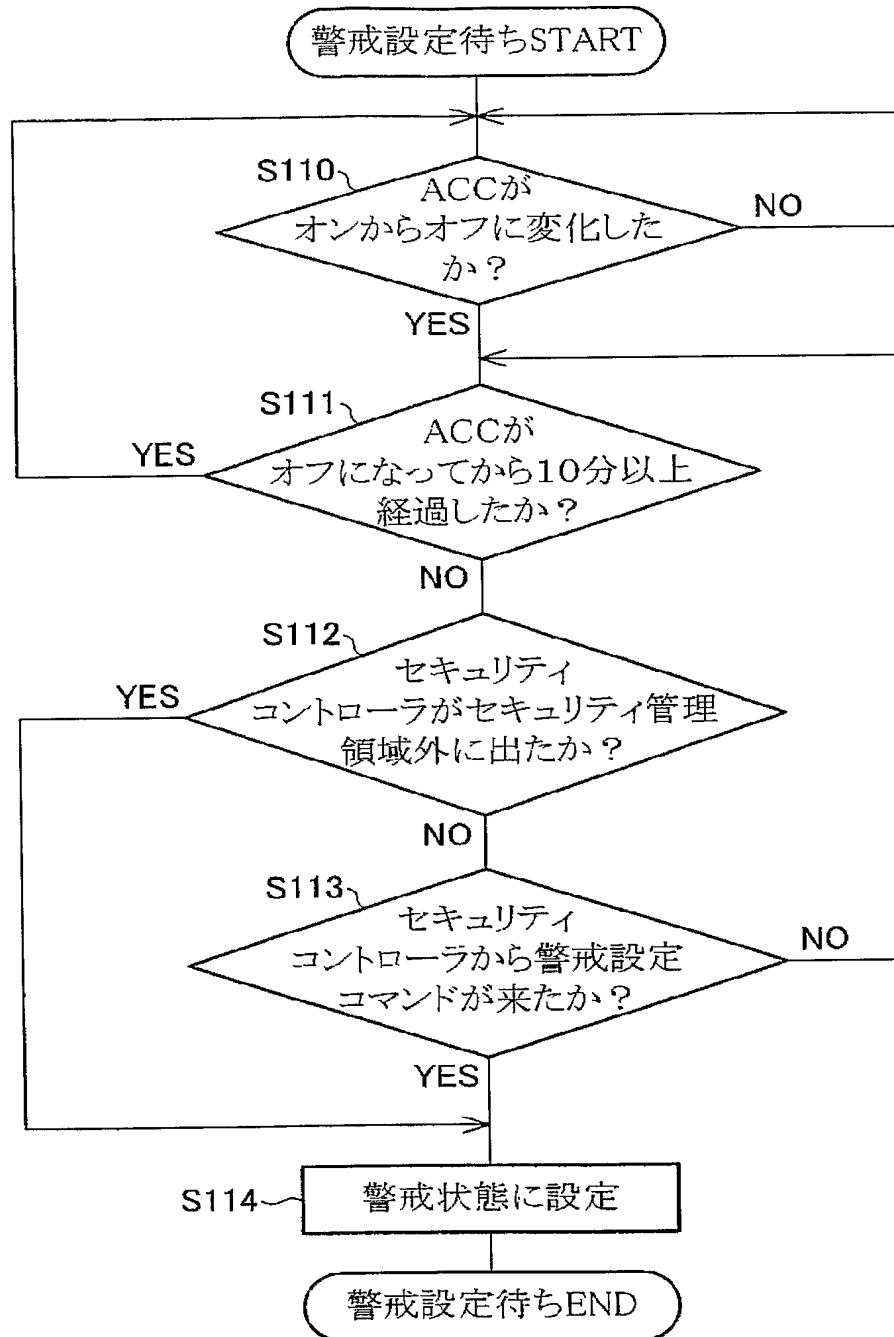
【図 6】



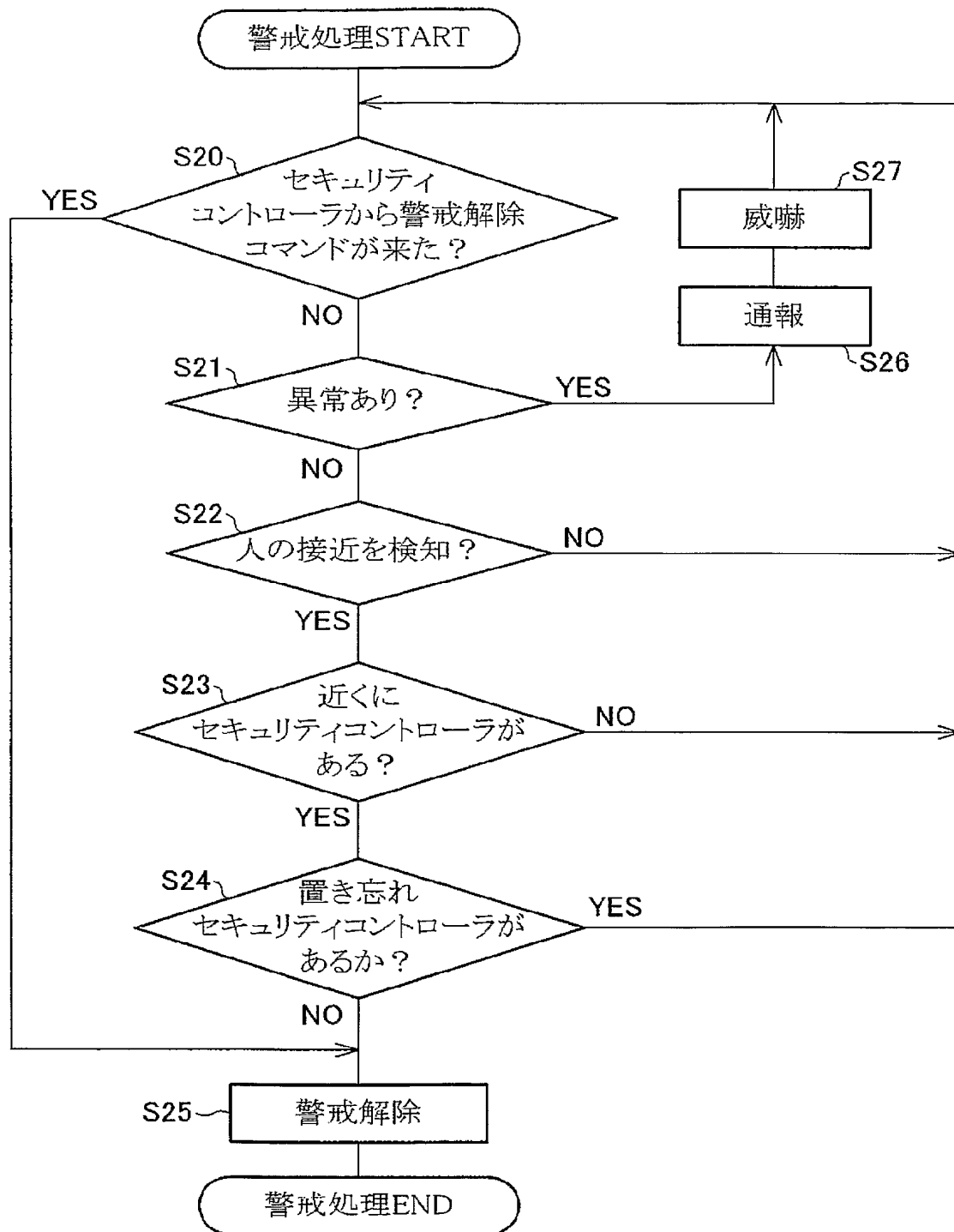
【図 7】



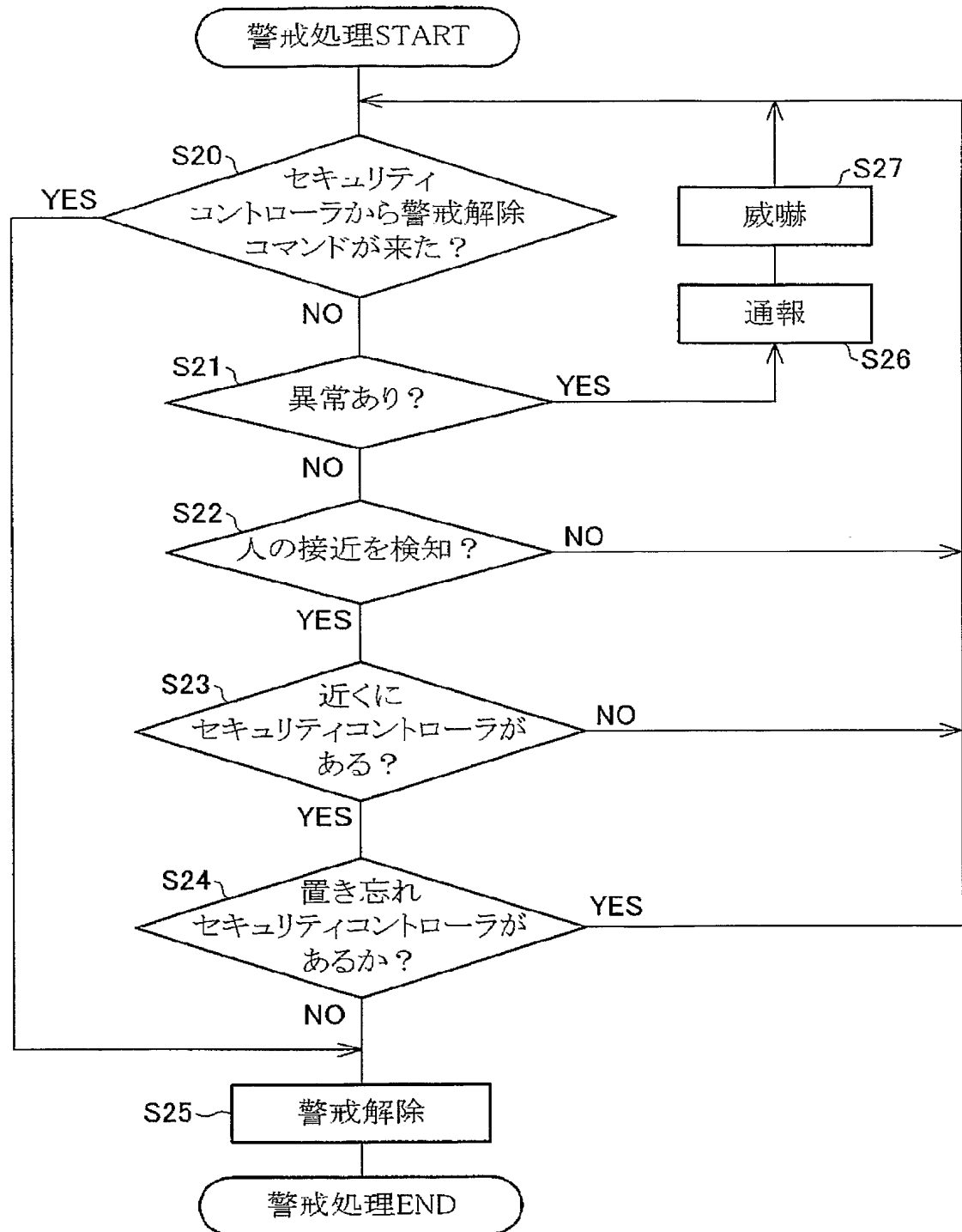
【図8】



【図 9】



【図 10】



【書類名】 要約書**【要約】**

【課題】 複数の情報送受信装置が情報処理装置に登録されている場合、当該複数の情報送受信装置の置き忘れによって生じる警戒状態の設定の誤操作を解消することを実現する情報処理装置を提供する。

【解決手段】 セキュリティ装置 2 は、セキュリティコントローラ 3 a ～ 3 c を所持したユーザのセキュリティ管理領域 5 0 に対する出入りを監視し、警戒動作の制御を行う。このセキュリティ装置 2 は、セキュリティコントローラ 3 a ～ 3 c それぞれと通信を行い、また、セキュリティコントローラ 3 a ～ 3 c それぞれの位置情報を取得する通信部、セキュリティコントローラ監視テーブル 3 0 を記憶する記憶部 1 1、セキュリティコントローラ 3 a ～ 3 c が所定領域内に置き忘れられたものであるか否かを判定し、自動的に警戒状態の設定または解除を指示するのか、ユーザの操作入力によって警戒状態の設定または解除を指示するのかを判定する置き忘れ判定部 2 6 を備える。

【選択図】 図 1

特願 2 0 0 4 - 1 0 6 9 4 6

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 2 9 4 5]

1. 変更年月日 2 0 0 0 年 8 月 1 1 日

[変更理由] 住所変更

住 所 京都市下京区塩小路通堀川東入南不動堂町 8 0 1 番地
氏 名 オムロン株式会社